2011

Educational evaluation of Cybersmart Detectives: final report: presented to the Australian Communications and Media Authority (ACMA)

Julian Dooley

Laura Thomas

Sarah Falconer

Donna Cross

Stacey Waters

Educational Evaluation of Cybersmart Detectives

FINAL REPORT

Presented to the Australian Communications and Media Authority (ACMA)

Prepared by the

Child Health Promotion Research Centre

Edith Cowan University

3 August 2011

Authors:

Dr Julian Dooley[1]

Dr Laura Thomas

Ms Sarah Falconer

Professor Donna Cross

Associate Professor Stacey Waters

Acknowledgements:

Narelle Alderman

Libby Alderman

[1] Dr Dooley is currently the Associate Director of the Sellenger Centre for Research in Law, Justice and Social Change in the School of Law and Justice at Edith Cowan University.

Table of Contents

List of Tables

List of Figures

Executive summary

The aim of the Australian Communications and Media Authority's (ACMA) Cybersmart Detectives (CSD) activity is to teach children key Internet safety messages in a safe school environment. The activity brings together a number of agencies with an interest in promoting online safety for young people, including education, State and Federal Police, government and child welfare advocates. The activity has been played by over 28, 000 students in Australia since initial trials in 2004.

Cybersmart Detectives is offered free to schools by the ACMA as part of the Australian Government's commitment to cyber-safety. Based on a real-world Internet safety scenario, the CSD activity is delivered to students in the classroom as a series of messages. Aided by the classroom teacher, students work in small teams, reading correspondence, voting on a series of poll questions and sending questions and suggestions to their 'Cybersmart Guide' waiting online. As the scenario unfolds, students discuss the risks of certain online and offline behaviours and ways of managing those risks.

Cybersmart Guides are an important part of the activity. Guides are teachers, police and Internet safety experts who help students throughout the activity. The Guides respond to questions and theories posed by students online and help guide teams through each of the clues. Along with the interactive online CSD activity, the ACMA also provides a suite of teaching resources to support ongoing Internet safety education in the classroom. These resources include lesson plans and access to other ACMA online and hard copy resources.

This independent evaluation, which was conducted by the Child Health Promotion Research Centre (CHPRC) at Edith Cowan University, was designed to answer five key questions:

1. Investigate if the game's key cyber-safety messages are identified by students;
2. Measure the short-term impact of CSD on student learning about cyber-safety;
3. Determine if students recognise the link between key cyber-safety messages and how these messages should be assimilated in their own behaviours/lives;
4. Examine the teacher's role in reinforcing the key cyber-safety messages; and

5. Assess the value of the pre-game and post-game lessons in reinforcing the key cyber-safety messages.

The evaluation used a mixed methods approach, comprising stakeholder interviews, teacher interviews, quantitative student data collection and focus groups with students enabling the triangulation of results to support the implementation of the CSD activity. In addition to the data collection and analyses described in the proposal, the CHPRC conducted supplementary analyses to explore students' responses to poll questions (embedded within the CSD activity) and qualitative transcripts comprising student and guide comments posed during the CSD activity.

Summary of key findings:

While an expanded section of the results pertaining to each research question is presented in Section 5, the following summarises the key findings and recommendations resulting from this research.

1. Risk group:

Students who were classified as high-risk (as a result of reporting fewer strategies to respond to unwanted online contact from a stranger) reported significantly more positive actions at post-test than at pre-test. This resulted in those high-risk students at the pre-test moving into a lower-risk group at the post-test. This result highlights the potential impact of the game on students who are the most vulnerable and at greatest risk for negative and inappropriate interactions online. Clearly, the game has important short-term implications in particular for those at greatest risk (***Key evaluation question 2***).

Furthermore, the CSD activity resulted in reported (intended) behavioural change (***Key evaluation question 3***). Students (in particular 11-year-olds) reported a greater intention to act after playing the CSD activity suggesting that participation in the game may have increased student's knowledge of the actions they could take to respond to contact by someone unknown to them. As noted, this is particularly the case for vulnerable youth.

2. Age differences

Several important age differences were found in this evaluation. For example, 11-year-old students reported significantly more positive actions at post-test than at pre-test when compared to 12-year-olds. Furthermore, 11-year-old students who reported having fewer positive responses if contacted online by a stranger at the pre-test demonstrated a significant increase in the number of skills at the post-test.

Interestingly, more than twice the number of 12-year-old students reported that they would talk to a teacher at the post-test compared to the pre-test (32% at pre-test compared to 68% at post-test). While it is unclear why this occurred, the large increase in the numbers of students who reported they would talk to an adult if contacted online by a stranger is very promising and highlights a positive but unintended outcome associated with the CSD activity.

3. Risk group profile

Several important differences were noted between the high- and low-risk students in relation to their use of technology and online activities (these are detailed in full in the results and discussion sections). Overall, high-risk students were more likely to interact with strangers online in a variety of contexts (e.g., social networking sites, chatrooms, online games). High-risk students used the Internet on their mobile phone more frequently than low risk students (one to three times per day, High: 15% versus Low: 9%, four to five times per day, High: 5% versus Low: 4% and more than 10 times per day, High: 5% versus Low: 0%). Furthermore, high-risk students reported more non-school related Internet use during the week, compared to low-risk students (e.g., about three hours/day – High: 10%; Low: 4%).

Although, fewer high-risk students (48%) than low-risk students (59%) reported using the Internet in an open area, similar percentages (22%) of students reported using the Internet in their bedroom. This highlights the importance of considering more than just the location of a computer when determining potential risks to cyber-safety.

More high-risk (73%) compared to low-risk (59%) students reported having a social networking site or instant messenger profile and using it for longer (14% of high-risk students

used it up to two hours a day compared with 8% of low-risk students). Importantly, more high-risk than low-risk students reported using online chat sites (66% versus 44%) or played games that involved other people (86% versus 65%).

In terms of their use of social networking sites, few differences were found between the risk groups. Of concern, more than half of students in both risk groups reported having friends online that they have not met offline (High: 57%, Low: 51%) with only 57% of high-risk and 44% of low-risk students knowing all or nearly all of their online contacts offline. In addition, a minority of students have not set their SNS profile to private (High: 39%; Low: 43%) and more than a third have shared their password with someone (High: 34%, Low: 43%).

4. CSD enjoyment factors

The majority of participants reported that they enjoyed the CSD activity. The key factors that students enjoyed more were explored with the majority indicating they liked the interactive nature of the game (i.e., answering questions and receiving feedback). Overall, the feedback from students and teachers was positive. The basic concept of using a computer game approach was appealing to young people as it was fun, engaging and contextualised their learning experience.

Teachers reported finding the game very useful and supportive of their offline activities (***Key evaluation question 4***). While some teachers felt their role was best suited to classroom management (with the assistance of cyber-safety experts to guide students online through game play), others enjoyed their role as a guide, seeing the importance of engaging with students online, a setting in which students interact daily. Unfortunately, few teachers implemented the pre- and post-game lessons, which accompany the CSD activity (***Key evaluation question 5***). The most commonly cited reason was a lack of time to do so. Those who taught the pre-game activities felt they were valuable in setting the scene for the CSD activity and provided useful background information on cyber-safety.

In addition to enjoying the game, students recognised the cyber-safety messages promoted in the CSD activity, as evidenced by both the quantitative and qualitative results (***Key evaluation question 1***). The particular messages that appeared to be salient with students included: reminding students not to communicate with others online whom they do

not know in person; awareness of privacy controls on social networking sites and the need for these to be set to private; awareness of the ease of identity deception online; age appropriateness of websites being accessed; and the importance of not sharing passwords.

As evidenced by the feedback from students and stakeholders, presenting safety information in the appropriate context is an important element of an effective approach to cyber-safety. Indeed, the majority of the teachers interviewed indicated that cyber-safety messages targeted to students using the CSD activity were very appropriate or appropriate given the role of technology in their everyday life. In addition, the role that the CSD activity (and similar cyber-safety resources) could play in supporting the content of other school-based cyber-safety strategies is important to highlight.

The CSD activity provides an opportunity to practice appropriate responding to inappropriate social interaction. This safe exposure to dangerous situations is, for obvious reasons, not easy to achieve. Despite young people being provided with relevant safety messages (i.e., stranger danger) from a young age, it is likely to be somewhat rare that they have an opportunity to practice personal safety in an ICT environment in a situation of immediate danger. Having opportunities to practice social problem solving skills in an environment that matches the environment within which these skills are likely to be used is a significant strength of the CSD activity.

1. Introduction

Technology has been fully incorporated into daily life and has become an integral component of the learning experience of all students. With the increase in availability and access to technology, much discussion has focused on the associated risks (see Dooley et al[5] for a comprehensive review of cyber-safety risks). Consequently, a great deal of effort has been put into developing resources that support and complement educational safety activities. However, to date, very few of the cyber-safety resources that have been developed have been subjected to systematic evaluation to determine the extent to which they promote, enhance or improve cyber-safety attitudes, awareness and practices. While a small number of evaluations have been conducted and published (see pages 22-35 for a review of the published cyber-safety program evaluations), the systematic examination of the effectiveness of cyber-safety programs has only just begun. This section will present an overview of several relevant theories and, given the limited literature on cyber-safety resources, will use related areas for illustration.

Through the rapid advances of technology today's youth are developing a high level of technical skills and, at the same time, showing preference for different learning styles as a result of new thought development[6-8]. Young people are growing up in a highly technological society and are far more able and experienced to process information rapidly than earlier generations and become easily bored at school if they have to 'power down'[8, 9]. What has resulted is the consideration of new educational approaches that incorporate technology that is engaging, empowers students to self-regulate, integrates more than one knowledge domain and promotes enquiry-based and discovery learning[10-12]. The use of games in education provides an engaging, interactive learning environment that increasingly challenges participants as they move through the levels and creates a balance between challenge, curiosity, control and fantasy[13, 14]. Games are often designed to be competitive and require taking risks which further develops problem-solving skills and increasing motivation [15].

Online games can be categorised in two ways; Personal Computer (PC) games and Net games. Within Net games there are Web, Network and Interactive online games. Web games require a website interface and registration by the player, such as the online game database 'Miniclip'. Network games (e.g., World of Warcraft), through the purchase and installation of software, allow multiple users on their own PC to play and interact through the Internet in a variety of gaming environments. Interactive online games (e.g., Habbo Hotel and Club Penguin) require logging into a server and interacting within a virtual environment[13]. The globalisation of games that now have an online web-based component and Net games now utilising instant messaging, chat rooms and in-game communication is providing gamers[2] with opportunities to interact, collaborate and communicate with other gamers in situations previously unavailable[16]. Virtual worlds are identified as social in character, enabling collaboration in several ways. The graphical representations of the gamers, through an avatar, aids in learning to consider others as part of a community and to interact with one another in the virtual realm[17]. Learning gains from virtual worlds are dependent on the teaching methodology used in facilitating learning in the school environment[17].

1.1 Educational games

As a result of increased exposure and use of Internet gaming technology, 'net-education' has arisen as a key component to reduce child and adolescent Internet risk behaviours. Research shows that young children lack adequate 'e-maturity' to handle risks associated with unsafe Internet use. For example, over 85% of Belgian primary school-aged children use the Internet in an unsafe manner[18]. Five distinguishable risk areas were identified: social relations such as the impact of cyber-bullying and cyber-stalking; emotional impact of pornography, violence and explicit language; physical health and the link to obesity and muscle pain; time management as a result of addiction and neglect towards other tasks; and consumerism and commercial exploitation[19]. A recent review provides a comprehensive overview of the available literature describing the prevalence, consequences and impact of engaging in and exposure to risks associated with the Internet[5].

There is emerging research examining the positive potential of gaming technology in education [20]. McFarlane et al.[21] stated that, the tasks and content of some computer games provide a forum conducive to learning, developing knowledge and skills resulting from game play. Funk[22] reviewed several studies and reported that games strengthen students' engagement, information processing, problem-solving, social development and

[2] Players of video or computer games

academic abilities. Educational scholars have argued that games can play an important role in childhood in psychological, social and cognitive development, also stimulating the players' internal motivation[23-25]. Educational games have the capacity to promote positive attitudes towards learning and school as a result of their engaging qualities[26-29]. In addition, educational games can promote cognitive capacity and functioning. For example, students learning curriculum through video games, compared to students taught through traditional learning methods, showed improved visual selective attention skills as well as an improvement in test scores[30, 31]. The potential for positive effects is greatest if the game overcomes the basic hurdle of being engaging for students and there is evidence that problem-based games result in higher student engagement than other types of games[32].

It has been suggested that video games allow for proactive and exploratory natures, encouraging students to investigate beyond the boundaries of selective material and allowing them to become self-reliant learners[33]. Games additionally have the potential to reach students who have low academic performance in traditional teaching and learning environments. Research suggests that computer-based game instruction has the potential for motivating, engaging, increasing attention and retention rate in children of all ages[34-36]. Case study research has shown that flexible, personalised, experiential and informal learning provided through online networks can be better suited to young people who are not engaged by conventional teaching methods[37].

Several disadvantages to computer game learning have been noted. Clark[38] highlighted several risk factors that can negatively impact on learning. Choosing a non-specific educational game may mean that the game objectives do not fall in line with learning objectives. Games may be distracting and students may concentrate more on scoring and winning as opposed to learning. Games developed for both genders may fail to impact them both to the same extent; disadvantaging either gender. Clark[38] also noted that a risk factor may be the hijacking of something students view to be personal and disconnected from school, causing them to feel patronised and alienated. The Becta Project[39] further proposed that games may also be: developed at incorrect levels of interest, challenge or degree of difficulty which can reduce motivation; be too long causing conflicts with time management as well as competing with children's attention span; poorly designed, addictive and gender specific; and designed for single use rather than collaboration further hindering developmental opportunities.

Effectively utilising video games as a learning tool can be diminished through complex controls, load time[3] and lack of educational support materials[40]. Consideration around training and support for educators needs to be given as obstacles may be faced through integrating the games into school curricula; hence, simulation-based environments have been reported to engage students and promote learning, lending itself to being further utilised in schools[13].

However, fully incorporating games into the educational experience of students can be difficult. In addition to system issues, resistance to incorporating games into the classroom can be based on teachers' ideals, lack of knowledge, level of skills and support available, and lack of effective educational programs[41]. Teachers' perceptions of games merely as entertainment, combined with a lack of knowledge and skills in computer-assisted instruction, have inhibited the introduction of this new technology into the classroom. Furthermore, the development of effective educational hardware and software has not matched demand which may also have provided some resistance to the positive incorporation of technology into the classroom[12, 42].

1.2 Theoretical evidence

Given that there are currently no relevant theoretical models specific to cyber-safety that can be utilised, it is necessary to identify appropriate theories from other areas, such as education. In this sense, relevant theories and models that specifically look at health behaviours and school-based interventions are useful to evaluate the success of a program and also predict or explain situations that arise. To inform the design of a successful health promotion intervention it is important to utilise a number of different theories throughout the various stages of project development[43, 44]. The Health Belief Model[43], Protection Motivation Theory[45], Capacity Building[46], Diffusion of Innovation[47], Health Promoting Schools Model[48], Coordinated School Health Model[49] and Positive Behaviour Support Model[50] all impact on the successful design, implementation and evaluation of video game use for educational purposes in school curricula.

[3] The time taken for a program or website to be in an executable or usable state.

The Health Belief Model (HBM) discusses factors believed to influence behaviour change in response to a potential health threat; including the individual's perceived susceptibility to the disease and assessment of perceived susceptibility to risks associated with the behaviour[43]. Therefore, applying the HBM to cyber behaviours provides a theoretical background into the use of educational computer games, specifically games that generate awareness of cyber dangers. The individuals' perceived severity of the threat also relates to the perceived severity of the risk (e.g., cyber-bullying or cyber-stalking). Finally, in the HBM, it is believed that through the actions of games, individuals would be encouraged or prompted to change their unsafe Internet behaviour, rendering the perceived costs higher than the perceived barriers.

Protection Motivation Theory (PMT) explains the motivational effect resulting from threat communications and is used to underpin fear arousal. It assumes that individuals are motivated to protect themselves from physical, social and psychological threats[45]. Similar to HBM, the perceived severity and perceived likelihood of the threat are examined and determine the perceived vulnerability. Coping ability is based on considering the recommended behaviours in two contexts. Firstly, the perceived effectiveness of the encouraged behaviour as a way to avoid or reduce the likely occurrence of the threat is considered. This is evident in developing safer behaviours that would avoid the likelihood of the threat recurring. Secondly, the individual completes a self-assessment of their ability to perform that behaviour (their self efficacy). Self-efficacy is a strong predictor of students' motivation and learning. Bandura's Social Cognitive Theory (SCT) [51] highlights self efficacy as a key component to successfully performing academic tasks and is a strong predictor of their abilities to accomplish that task[52, 53]. It determines whether behavioural change will result as the belief that the desired effects will be produced by a person's actions. This belief is a strong incentive for behavioural change. SCT affects whether people mobilise motivation and perseverance needed to succeed, how they recover from failures or relapses and how that change in habit is maintained[25, 51, 54]

Capacity building relates to the development of knowledge, skills, commitment, structures, systems and leadership, and is a key component in effective interventions[55-60]. To effectively integrate video game education into classrooms, schools need to address material resources, staffing, funding, time, facilities, staff training and external agency assistance to build school capacity. In accordance with this, the Positive Behaviour Support Model (PBS) supports systems change approaches focussing on behaviour modification at

all levels from the school to the individual[50]. The steps outlined below illustrate a clear pathway to ensuring successful adoption of interventions. First, a school must show commitment by providing training to initiate and continue the process facilitating ownership of the intervention. Second, schools need to generate opportunities to reflect on the experience, providing effective evaluation of participation, ongoing developments and analysis of outcomes. All of this information should be used to inform action plans to manage concern points[50, 61]. The Diffusion of Innovation supports the PBS steps through its four stage process of adoption: dissemination or awareness; adoption; implementation; and maintenance[61-63]. It is important that educational games seek to address these four processes to be effective.

It is critical that schools implementing interventions (including health promotion interventions) are engaged in the Health Promoting Schools Model, which links education with health[64]. Characteristics include a formal curriculum that develops a wide variety of skills, school ethos, physical environment that is safe and comfortable, school policies that reinforce guidelines developed by staff, students and parents, school health services, school-home-community interaction and organisational structures that set priorities and develop plans around resources and professional development[48]. Although not directly related to cyber-safety, it is clear that these same processes would form integral components of any school (including at a sector and governance level) attempts to enhance the safety of students online. Similarly, the Coordinated School Health Model builds on key concepts developed in the Health Promoting Schools Model and focuses on the physical, emotional, social and educational development of students. It highlights the need for health, physical education, health services, nutrition, inclusion of staff and community involvement to ensure the school is united on health promotion interventions[49]. These two models are not dissimilar and provide steps and components for schools to introduce further health promotion in their own environments.

1.3 Elements of engaging computer games

Engaging online (and computer-based) educational games need to reflect both theoretical and realistic needs and values relevant to the target audience[65]. Therefore, to create engaging learning opportunities, computer-based games should take into account factors such as gender differences and preferences, and be suitable for use within the constraints of various educational environments (e.g., technological capabilities and

classroom design) [66]. Specifically, game content and feedback should be challenging enough for students to be cognitively and emotionally engaged whilst also being aligned with school curriculum and learning outcomes. The associated teacher guides should also provide activities and resources that align with these learning outcomes and the logistics involved with game play should also reflect classroom time constraints and realities[8, 67, 68]. Further, the design of such games requires several learning principles and techniques to encourage play and capture user's (player's) attention. In particular, the following factors were identified as key in engaging adolescents in computer games:

- The ability for the user to modify game mechanics to customise the experience (i.e., player roles) to increase the sense of ownership [8, 10, 53, 67, 68].
- Integrate a sequential narrative and storyline, including clear goals and objectives as a rationale for the game [8, 10, 41, 67-69].
- Use a suitable level of complexity, challenge, problem-solving, competition and consolidation so the user is required to think laterally and gain a sense of victory when provided with results and feedback on outcomes [8, 10, 41, 67-69].
- Incorporate information such as game rules and instructions to inform the constraints of game play [10, 41, 53, 67, 68].
- Integrate a sense of fantasy and meaning that are independent from physical laws (i.e., can fly) [10, 67-69].
- The ability for players to interact/play against others in real time [8, 10, 67, 68]. This component distinguishes online games from traditional computer and video games [70, 71].
- Create a high speed, immersive sensory environment with a rich variety of graphical representations to support a wide range of player options and scenarios [41, 53].

Overall, a review of the educational literature makes it possible to make a few key recommendations to ensure that the game is successfully integrated into the curricula and achieves the goal for which it was designed. It needs to be balanced between academic content, game rules, legitimate participation and framing narratives [34]. Several authors (e.g., Rosas et al. [41]; Paraskeva, Mysirlaki & Papagianni [72]; Shih et al. [15]) note that to be an effective instructional tool, games need to have several key elements:

1. The challenge needs to be clear, meaningful and comprised of uncertain outcomes, varying difficulty levels and randomness;

2. Constant, instant feedback keeps students engaged and scaffolds, such as clues, encourage continued playing and can aid performance [72, 73];
3. Game goals and tasks need to be precise with clearly outlined rules and meeting the educational, developmental and instructional level and goals and of the target audience;
4. There needs to be a level of fantasy where the character, who the student plays as, must be clearly identifiable with them and be emotionally appealing linked directly to the activity and sensory, and cognitive curiosity need to be engaged [14, 28, 74, 75]; and
5. Activities need to be as authentic as possible within the environment of the game with a high level of exploration within the game to use different strategies and aid in the student developing self-reliance in their learning [15].

1.4 Cyber-safety program evaluation

Importantly, the focus of this evaluation is on cyber-safety educational resources. As such, it was critical to conduct a thorough review of the scientific literature to identify any evaluations that were similar in nature to the current study. The literature review method described below was conducted every 2 months (December, 2010; February, 2011; April, 2011) to ensure that the information was as up-to-date as possible (the results of the April search are reported here). The following methodology was used:

A brief literature review was conducted in the Scholarly databases available to Edith Cowan University. Specifically, education (Academic OneFile; Proquest 5000 International; WilsonWeb; and ERIC), health science (CINAHL; MEDLINE; PsycINFO; and SPORTDiscus), and social science (Family and Society Plus) databases were searched. The World Wide Web (Google) was also utilised a search engine for academic and grey literature. The academic literature included peer reviewed journal articles listed on the Cochrane database, while the grey literature comprised electronic publications, reports, theses and expert opinion. The reference list of each available article sourced in the aforementioned literature search was snowballed for further articles that may have been missed in the initial literature search. Key search terms included ‘evaluation of a cyber-safety game’, ‘evaluation of online games’, ‘gaming technologies and behaviour’, ‘social marketing and message uptake’, ‘social marketing and message recall’, ‘gaming and product

placement', 'social marketing and theory', 'cyber-safety and theory', and 'gaming and behaviour change'. In addition, the resources currently held by the CHPRC (e.g., the cyber-safety literature review prepared for the Department of Broadband, Communications and the Digital Economy) were consulted and reviewed for relevant sources. Furthermore, a comprehensive search of the gray literature was conducted in an effort to identify government and non-government reports and white papers detailing evaluations of programs that centred on cyber-safety.

The literature search revealed a large number of articles (more than 2,000) that were on related topics (e.g., general discussion of cyber-safety risks in youth samples) but very few that were focused on cyber-safety program evaluation. In the most recent search, we located a study that systematically reviewed the available evidence on cyber-safety program evaluations [76] (see Mishna, Cook, Saini, Wu & MacFadden [77] for a more complete review published in the Campbell Systematic Reviews). Mishna and colleagues took a broad approach to cyber-safety by including all studies that were classified as addressing cyber-abuse. In this review, the authors included cyber-bullying, cyber-stalking, harassment, sexual solicitation and exposure to pornography. Their initial search revealed 3,029 related studies of which three met their inclusion criteria. Two of the studies (I-SAFE and the Missing cyber-safety program) were evaluations of child and adolescent targeted psycho-educational interventions designed to address Internet safety knowledge and online risky behaviour; the third (a review of the HAHASO anti cyber-bullying program) was an unpublished doctoral dissertation and was not included in the review. In addition to these studies, a small number of other studies (published and unpublished reports) were identified.

Given the limited available evidence, all of the studies that were located as part of this review will be presented separately.

1.4.1 I-SAFE program evaluation

The I-SAFE program was developed in the USA in 1988 and aims to educate young people on safe use of the Internet use (more information available from www.isafe.org). The program originally aimed to educate and enhance cyber-safety for all students. It comprised three core components: an education component which consisted of a school-based curriculum for K-12 aged students; an outreach component which utilized abilities and

resources from various groups including community and school leaders, parents, and students to increase Internet safety awareness; and the final component, the Youth Empowerment Campaign, which utilized peer-to-peer communication methods as a means to disseminate Internet safety messages.

> "i-SAFE America is committed to keeping abreast of changes in technology, law, and youth trends and updating the curriculum as appropriate. As such, in 2004-2005, the curriculum was revised again, based on teacher feedback. This version of the curriculum includes the same five core lessons described in the revised curriculum (also see Appendix 13 [of the evaluation report] for more detail), with slight changes in wording, order and activities. The main difference between the revised and 2004-2005 versions is the inclusion of optional PowerPoint presentations for each of the five core middle school lessons. These optional PowerPoint presentations were updated to include pauses for class discussion and activities and are intended to help guide the lesson. In addition, the program now also includes several supplemental lessons for fifth through eighth grade on cyber-bullying, literacy, and homeland security that are available online for interested schools. Finally, i-SAFE began publishing a regular newsletter that is available on its Web site to help keep teachers up-to-date on Internet safety."
>
> Description of 2004-2005 revised curriculum [2] (p.6)

The original program was revised and broadened in 2004 to include five core lessons. The lessons that are part of the program include: Community, Cyber Security, Personal Safety, Predator Identification, and Intellectual Property. The curriculum was expanded to include multimedia activities and youth empowerment activities and these activities change depending on the target age. Several elements of the program have undergone revisions somewhat in line with technology developments. For example, additional components have been added to the K-4 program, called I-Buddy, while webcasts have been added to the high school program. Using a train-the-trainer model, the organisation collaboratively works to develop an implementation plan with a school or district. This helps in standardising the implementation of the program.

The evaluation of the I-SAFE program was conducted in 18 schools (12 exposed to the program and 6 control) to answer three key questions [2] (p.9):

1. Do students retain the knowledge received during i-SAFE lessons?

2. Do they use this knowledge?
3. At what reduced levels or intensities of implementation are program benefits no longer measurable?

Positive and significant changes in knowledge between the treatment and comparison groups, both on average and over time, were reported. Furthermore, several factors (e.g., gender, computer skills, and parental supervision) were more likely to have an effect on knowledge. Importantly, the results for behaviour change were not as positive. Given the difficulty demonstrating behavioural change, it was unsurprising that no significant behavioural changes between the treatment and comparison groups were reported.

Several interesting results were presented which are relevant to the current evaluation. For example, a significant gender difference was reported in relation to knowledge retention; boys retained less Internet safety knowledge than girls over time. In addition, younger students retained more Internet safety knowledge than older students. Further, the same gender and age pattern was found for predator identification and intellectual property theft (downloading media without paying for it). In addition, a gender difference was reported in relation to perceiving and managing risk with boys perceiving fewer risks associated with interacting with others online. Consistently, boys reported sharing more personal information with people they met online than did girls. Interestingly, this pattern was reversed in relation to information provided in emails; girls tended to include more personal information in email usernames than did boys. Finally, the authors reported a positive relationship between the number of hours the program was implemented and the amount of knowledge gained; the more time that was spent on the program the greater the extent of knowledge gained in relation to general Internet safety, predatory identification, managing risk and sharing personal information. However, they did not provide an indication of the level at which program implementation was deemed to be optimal (i.e., the number of hours at which the program was most likely to be implemented that resulted in the greatest knowledge gains).

1.4.2 Missing Program evaluation

The Missing Program is a Canadian based resource aimed at enhancing the cyber-safety skills of 11-14 year olds using a multi-pronged educational approach. At the time of the evaluation conducted by Crombie and Trinner [3], the full resource kit consisted of an

interactive, online game, a documentary video about Internet crimes, a poster and brochure and a website[4]. A review of the manufacturer's website revealed several additions to the Missing game including the production of a game, Mirror Image, targeted at 14-16 year olds.

> "The game, which is based on a true story, clearly illustrates some of the tactics used by people who use the Internet to victimize children. Children playing the game assume the role of a police officer and solve a series of puzzles in order to track down a missing teenager. This unsuspecting teenager leaves the country with an Internet predator he met in an open chat room. Players of the game have the chance to see how this Internet predator successfully capitalizes on the teenager's vulnerabilities and uses various tactics to gain his trust and to lure him away from home. The game contains the message that revealing personal information about oneself on the Internet can make one vulnerable to Internet victimization. In addition, by showing children how this Internet predator misrepresented himself, the makers of the game attempt to convey to children that they cannot necessarily trust what they are told by people they have met online."
>
> Overview of Missing game [3] (p. 10)

The evaluation conducted by Crombie and Trinner evaluated the effectiveness of the Missing game with students in Grades 6 and 7 in eight elementary schools in Vancouver, Canada. The authors administered the game to 50% of classes in six of the eight schools (forming a "treatment" group) with the remainder being used as a comparison group. The authors used a pre/post design where baseline assessments were taken, the game was administered and, approximately three weeks later, a post-test assessment was conducted. This enabled the authors to examine group differences across a variety of variables including open chat room conversations, e-mail communications with someone originally met on the Internet, personal Web page design and meeting in person with someone originally met on the Internet. These will be addressed separately for clarity.

[4] More information about the Missing kit can be found at http://www.livewwwires.com

Open chat room conversations: Students more frequently reported visiting open chat rooms at the pre-test than the post-test. However, this difference was the same independent of the group (i.e., treatment or comparison) or gender suggesting that exposure to the game did not impact on students reported use of open chat rooms. The authors reported that there was a significant difference between the treatment and comparison groups in relation to disclosing some personal information (gender, age, school name and city). Importantly, group differences in the tendency to disclose gender and age was related to an increase in reporting in the comparison group at the post-test assessment rather than a decrease in the treatment group. However, there was a decrease in the reported incidence of sharing school names and city by the treatment group (relative to the comparison group) in open chat rooms, which the authors attributed to playing the game. Interestingly, the authors reported some gender differences in relation to information sharing in open chat rooms. Specifically, boys were more likely to share their personal email address with strangers than were girls.

E-mailing someone originally met online: No differences were reported between the treatment and comparison groups in relation to the incidence of e-mailing a person originally met online that can be attributed to playing the game. The treatment group reported a lower incidence of this action at both the pre-test and the post-test. However, there were differences over time with more students at the post-test than at the pre-test indicating that they would not e-mail someone they had originally met online. As with open chat rooms, it appeared that males in this study engaged in more risky behaviours by e-mailing strangers more frequently than females.

Personal web page design: This issue focused on the type and extent of personal information sharing on personal web pages (web pages they had "either already designed or that they might design in the future", [3] (p. 18). Interestingly, the authors reported that participants in the comparison group were more likely to share personal information (i.e., school name) at the post-test than the pre-test. This was not the case with the treatment group. The authors suggested that this result may relate to the effect of exposure to that concept at the pre-test phase but it is unclear how this process may work. A number of gender differences were noted. Specifically, females in the treatment group were less likely to report posting their age or a picture on a web page. However, the differences between the treatment and comparison group was evident at both the pre and post-test assessments and, therefore, can't be attributed to exposure to the game.

Attitudes related to Internet safety: Eleven items were used to assess attitudes about Internet safety: How truthful are people when they talk online?, How likely is it that someone online would pretend to be someone else?, How likely is it that someone online would try to manipulate you?, How much can you trust people online?, How long do you have to know people met online before trusting them a little?, How long do you have to know people met online before trusting them a lot?, How likely is it that someone online would try to lure you away from home?, How likely is it that someone online would try lure someone your age away from home?, How risky is it to disclose personal information in an open chat room?, How risky is it to disclose personal information in e-mail to someone met online?, and How risky is it to disclose personal information on a personal Web page?

The authors noted that, for the safety-related attitude items they assessed, there were "no significant results indicating a positive effect of the Missing program on changing these attitudes for the sample of Grade 6 and 7 students" [3] (p. 28). As with the other issues addressed in the evaluation, there were gender differences apparent in relation to this topic; females reported overall safer attitudes than males for nine attitude items.

Overall, the mixed results of the Missing game evaluation did not provide strong evidence of the effectiveness of the game in increasing and enhancing cyber-safety practices of students aged 10-14 years. The authors used a strong methodological approach to evaluate the game and the results could be an accurate reflection of the impact of the game or it could highlight the challenges associated with cyber-safety program evaluation.

1.4.3 Child Exploitation and Online Protection (CEOP) Centre ThinkUKnow programme evaluation

The ThinkUKnow (TUK) program was developed by the CEOP Centre as part of their strategy to address the harm associated with the misuse of technology and the risks to young users. The focus of the program centres on three key messages: how to have fun, how to stay in control and how to report a problem. The TUK program aims to enhance safety by informing users (and their parents/carers) of the risks associated with technology and bridging the gap between older and younger users (often referred to as the "digital divide"). In 2010, TUK expanded to Australia in a collaborative effort involving the Australian

Federal Police and Microsoft Australia. The approach taken with TUK involves lectures and presentations given by trained presenters (including youth presenters) to schools-aged students. In addition, a series of multimedia and hardcopy resources have been developed (which are available at www.thinkuknow.org.au).

Davidson et al [78] examined several aspects of the TUK program including the extent of online risk-taking, the effect of the safety advice and an overall evaluation of the program. For clarity, these will be presented separately. The mixed methods study included 1,718 students aged 11-16 years of age from seven schools in the UK (England, Scotland, Wales and Northern Ireland). Nearly 60% of students (*n* = 1,028) were recruited from schools while the remainder (*n* = 690) were recruited online.

Extent of online risk-taking: The results of the TUK program evaluation revealed that many children reported engaging in risky behaviour (e.g., interacting with strangers online) and would continue to do so. One in five children reported experiencing a threatening experience online, which was defined as being made to feel uncomfortable or being bullied. Not surprisingly, there was a statistically significant (but small effect size) association between interacting with strangers and higher levels of experiencing threatening situations. Finally, although girls were at higher risk than boys, boys were twice as likely to do nothing in response to being victimised.

Effect of safety advice: The authors reported some interesting results in relation to the source and implications of safety advice. For example, parents/relatives and schools were the most commonly reported sources of safety information. Furthermore, while there was evidence that the key Internet safety messages were being retained by children, there was little evidence that these messages were put into practice and this was especially the case for the 13 year and older group. Consistently, students in this study reported that safety advice had little impact on their past or planned risk-taking behaviours.

Several interesting (and concerning) results were reported in relation to interacting with strangers. For example, young people who had received safety information in the past two years were just as likely to interact with strangers online but less likely to share certain

personal details (e.g., home address). So, while there was a positive change in relation to sharing information there was no change in relation to interacting with strangers. The authors asked these questions regarding interacting with strangers in the context of instant messenger (IM) chat and Facebook (social networking sites). Thus, while young people (in this study) reported being less likely to share personal information with strangers, the fact that they were just as likely to interact with them potentially means that these unknown people could have access to some personal information regardless of if it is shared directly in the context of a conversation (e.g., by viewing their Facebook profile page). Young people also reported that they were aware of what they should do in response to a threatening situation and that they were unlikely to do nothing if threatened. Interestingly, young people who have had the TUK training reported being more likely to report a threatening experience online. Despite this, the authors reported that there was no evidence that the TUK training or website reduced the likelihood of sharing personal information or interacting with strangers.

Evaluation of the TUK program: In terms of the effectiveness and impact of the TUK program, two key findings are of interest. First, a high proportion of young people were unable to recall whether or not they had been exposed to the TUK program. Second, the recall of safety messages in young people fades over time with less than half of young people who have been exposed to the program indicating that they remember the messages well (there is no evidence that the authors measured actual message recall over time).

Overall, there appears to be some clear benefits associated with the TUK program. However, some concerning results were also noted. Most importantly, the suggestion that young people did not report a change in their inclination to limit interactions with strangers regardless of their exposure to a cyber-safety program clearly warrants further investigation. Davidson and colleagues [78] reported several supportive results highlighting the need to better understand the ways in which young people engage with friends and strangers online. It may be that these results (in relation to interacting with strangers) relates to the way in which young people define strangers and how they view technology as a social tool, that is, a mechanism to interact socially with other people.

1.4.4 NetSmartz evaluation

The NetSmartz program was developed by the National Center for Missing & Exploited Children as an interactive, educational means to provide age-appropriate resources to help teach 5-17 year olds about on- and offline safety. This multi-media program targets children, parents / caregivers, educators, and law enforcement.

"NetSmartz goals:

1. Educate children on how to recognize potential Internet risks.
2. Engage children and adults in a two-way conversation about on- and offline risks.
3. Empower children to help prevent themselves from being exploited and to report victimization to a trusted adult." [1]

Two schools were selected by the NetSmartz Program Manager and surveys were administered to 122 students (24 students from Grade 3 in one school and 98 students from Grades 3-7 in another). Data was collected on two occasions prior to and after participation in the NetSmartz program. The authors reported the following:

⇒ An increase from pre-test to post-test in the number of students who reported they believed it was unsafe to meet someone in person after chatting online (54% versus 83% respectively).

⇒ An increase from pre-test to post-test in the number of students who reported they believed it was unsafe to post their picture on the Internet (25% versus 98% respectively).

⇒ An increase from pre-test to post-test in the number of students who reported they believed it was not safe to tell someone their real name (20% versus 98% respectively).

⇒ An increase from pre-test to post-test in the number of students who reported they believed it was unsafe to put their address on the Internet (25% versus 88% respectively).

Despite these results, the small and biased sample size (in addition to the purely descriptive statistics presented), limits their generalisability and interpretability. The authors (p.1) reported that "participation in the NetSmartz program increased the children's awareness of Internet dangers and allowed them to be more comfortable and confident Internet users." However, based on the data contained in the report, it is unclear on what grounds this conclusion is made. The authors do note that the majority of students (79% in one school and 82% in the other) reported that participating in the NetSmartz program will change the way they do things on the Internet but there was no objective measure of this (i.e., what students actually did).

1.4.5 Net-Detectives evaluation

The Net-Detectives[5] role-playing game is part of the Kidsmart resource developed and produced by Childnet International, a UK-based charity. The game is based around a hypothetical situation where a teacher receives an anonymous message in relation to a female student, Tiffany. The message conveys to the teacher concerns about Tiffany's recent behaviour. Over the next 90-120 minutes, students are presented with a series of messages and clues, which they use to solve the case. The game provides students with an opportunity to interact with experts and law enforcement officials. Given the similarity between Net-Detectives (ND) and Cybersmart Detectives[6], this evaluation will be reviewed in detail.

Wishart et al [4] used a mixed-methods approach (using quantitative and qualitative methods) to determine (1) if students aged 9-12 would engage with an online role playing game, (2) if students would receive and remember key Internet safety messages, (3) what factors might detract from this approach to learning, and (4) what strategies would best support the delivery of an online role playing game in schools. Initially, an email questionnaire was distributed to 263 schools that were provided by the Kidsmart team and included schools who had not yet used the resources. This resulted in forty-nine responses of which six schools were using ND. The authors also conducted telephone interviews with

[5] According to their website (http://www.net-detectives.org/index.html), this Childnet International project is no longer active when accessed on April 24, 2011.

[6] The content of CSD was based on Net-Detectives.

twenty-six teachers (two of whom were using ND), student observations in three schools, focus groups with teachers and collected quantitative data from students post-observation.

The authors reported that while the awareness of ND was relatively low (only 21% of participants reported visiting the website), among those who did the rating of the game's effectiveness was high. For example, 75% of teachers reported that the game had an "great deal of impact on the intended audience's awareness of Internet safety issues" [4] (p. 465). Although most teachers who were interviewed indicated that elements of the game were helpful, a variety of reasons were provided including: based on a real-life scenario, encourages exploration, enables open discussion, engaging and being part of a larger group online.

Teachers were also interviewed about their attitudes and experiences with the ND game. Only six out of thirty-seven teachers had any experience with ND and only these have been included in the evaluation report. Participants reported that they believed the game enhanced the students' learning experience, supported students' discovery learning and encouraged physical involvement and engagement. Of interest, Wishart et al [4] reported a wide range in the extent to which teachers prepared for the administration of the game with their students. For example, in one school, teachers did not prepare their students at all while in another the students were so prepared they knew the outcome of the game before commencing the activity. In addition, technical difficulties were experienced in two of the schools where the game was administered which resulted in a delay in the amount of time taken to respond to student questions. Although it was not clearly addressed, these difficulties may have resulted in less than 17% of student questions being responded to in two of the schools where the game was administered. The authors reported that "Childnet reports that the normal percentage of questions responded to in previous activities (albeit conducted in KS2 [Key Stage Two schools with pupils aged 8-11 years] schools) is about 75%. They were unprepared for the number of teams per school and the rate at which the older pupils typed. Also many of the children's questions were inappropriate or unanswerable" [4] (p. 468).

In addition to the above data collected, the authors also administered a quantitative questionnaire to student participants. This questionnaire reflected student's opinions about

a variety of game related issues but does not reflect the extent to which the game changed or impacted on those opinions. In addition, the lack of a pre-test (or baseline) assessment makes it impossible to gauge the extent to which some factors may or may not have been impacted by exposure to the content of the game. For example, it may be the case that participating students knew not to give out their personal details before playing the game. Nonetheless, several interesting results were reported by Wishart et al [4].

Students that participated in the evaluation reported that the most important things they learned as a result of playing the game included: don't give out personal details (37%), don't trust what people say in chat/on the Internet (27%), avoid chat/some Internet sites entirely (14%), don't meet up with people from chat rooms (7%), chat rooms and the Internet can be unsafe (6%), and various other responses (12%). Among the things students liked best about the game were: interacting with experts (28%), solving clues and being a detective (23%), learning about safety on the Internet/in chat (11%), the story line (7%), it was fun (6%), seeing each others' and other schools' messages (5%), not much/wasn't one (3%), and various other responses (17%).

Furthermore, when asked what factors or components of the game assisted students to learn about cyber-safety, the most common response was the story itself (43%). Other factors included: a safety point from the story (31%), nothing (7%), responses and messages from the Action Centre (6%), the seriousness of the consequences (3%) and a variety of other responses (10%). The relatively low percentage of students who reported learning from the responses and messages from the Action Centre (i.e., ND staff) is likely related to the low rate of response to student questions (910 responses to 5413 questions) rather than the content and usefulness of the responses.

Not surprisingly, the most commonly suggested area for improvement in the game related to increasing the speed and number of replies to questions (54%). Additional suggestions included: increasing the speed at which the activity unfolded (11%), no improvement necessary (5%), have more things to do (4%), make it easier to understand (3%), and a variety of other responses (23%). The speed of the activity (or lack thereof) was

an interesting issue and one that appeared to decrease the sense of engagement for students[7].

"The following recommendations for hosting an online role play based around Internet chat in UK schools are suggested by this study.

- Preparation of teachers can be improved by providing step by step instructions about how the activity runs, to include screen shots or a simulation.
- Clear directions should be provided for teachers about how to induct their pupils into the activity to include preparation for role, guidance on types of questions to ask and on expected number and frequency of replies.
- The number of teams per school needs to be set beforehand so that the host can assign suitable resources.
- Consideration should be given to the introduction of a system to triage questions.
- Consideration should be given to fitting the activity into a maximum of two periods, including time allowed for briefing and a plenary (say a maximum of 80-90 minutes online). Alternatively, restructuring for a series of three 50min periods with one for briefing and one for the plenary may be more acceptable.
- More activities need to be included for pupils to carry out whilst waiting for replies to their messages.
- Consideration should be given to having the pupils play a role that they can immediately identify with, perhaps "a friend of a similar age".
- Pupils should be able to access previous as well as current messages."[4]

(p. 472)

[7] The game administration took approximately 2 hours and there were often long delays while waiting for the next message and replies to questions (Wishart, 2007).

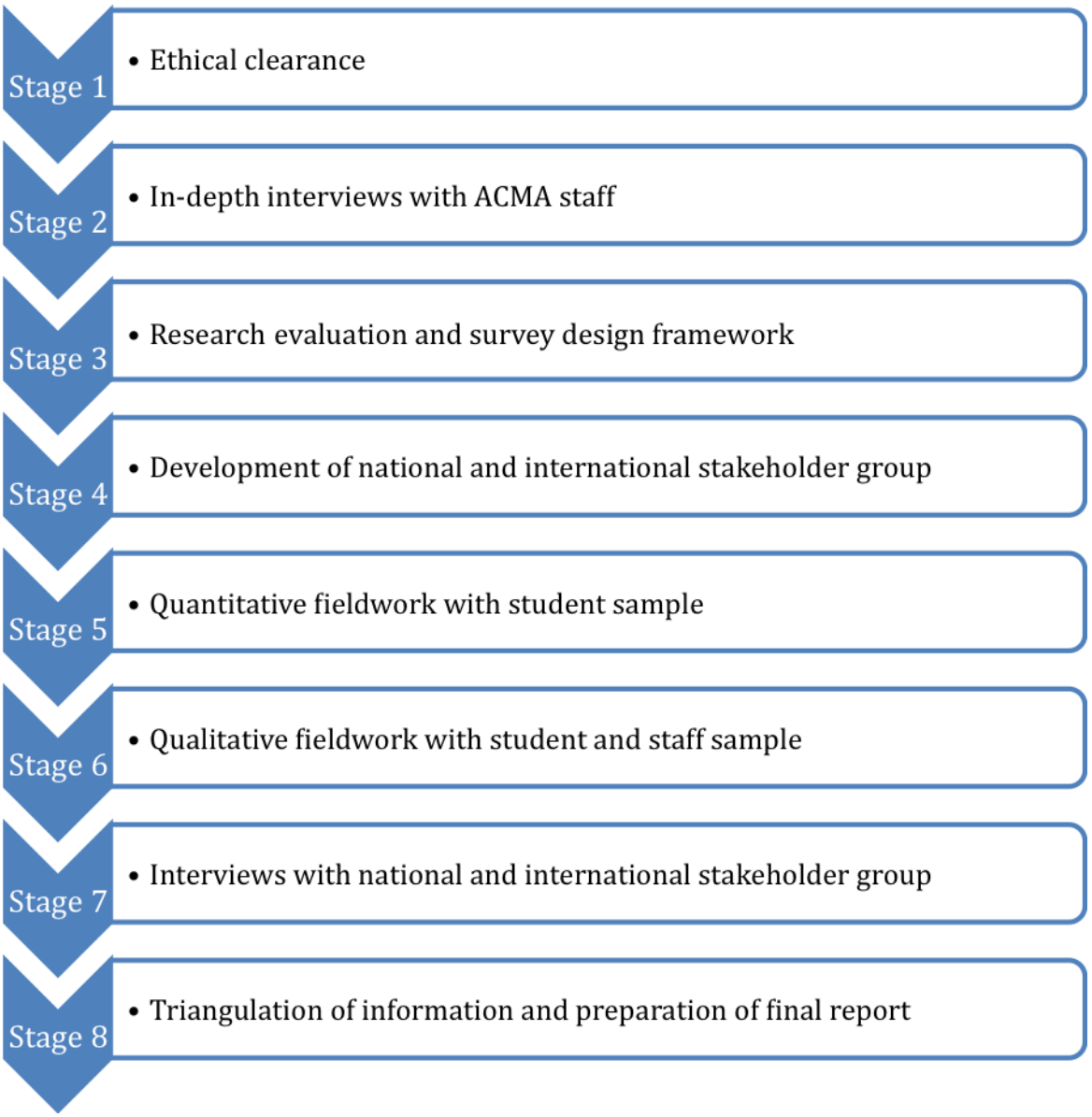
Overall, the authors reported that “all sources of data collected in this study agree that a number of benefits arise from participation in the Net-Detectives online role play” [4] (p. 472). Several suggestions were offered in relation to hosting online role play and these are presented in the text box above. Despite the benefits and advantages reported by the authors, the lack of data supporting any change associated with exposure to the game is a limiting factor.

The results of several cyber-safety program evaluations have been presented to provide an overview of the evidence outlining the effectiveness of these programs. Overall, limited evidence has been provided to date supporting the effectiveness of any cyber-safety program and, in particular, the evidence-base of the programs currently available. The evaluations discussed above had methodological limitations restricting the extent to which the results can be interpreted with confidence. Importantly, Mishna and colleagues’ [76] review (using strict methodological inclusion criteria) resulted in only two program evaluations being considered. Nonetheless, the reviewed evaluations have important results, which can be used to guide the development of cyber-safety program evaluation. As such, the evaluation of the Cybersmart Detectives (CSD) activity was developed using a multi-informant, multi-method, multi-phase and multi-methods approach (see Figure 1 below) in order to obtain a comprehensive variety of data to examine the effectiveness of the CSD activity and significantly contribute to the evidence-based evaluation of cyber-safety programs.

1.5 Evaluation Framework

The CSD evaluation was completed in eight major phases (Figure 1 below), some of which ran concurrently. The full extent of research activities completed during each phase below is described in the methods section below. The approach to evaluating the CSD activity was chosen to provide the most useful data that could be collected within the time and financial constraints.

Figure 1. CSD activity evaluation framework



2. Background

The CHPRC conducted in-depth interviews with ACMA staff involved in the development and implementation of the CSD activity to gain an understanding of the game and its implementation, as well as the level of support provided to and feedback obtained from schools. Five ACMA staff were interviewed as part of this knowledge gathering strategy. Information attained from these staff are presented here as background information to the evaluation.

2.1 Game history

Cybersmart Detectives is an adaptation by the ACMA of a similar game developed by ChildNet International which is a not-for-profit organisation based in the United Kingdom[8]. The original version ran for two hours, was established for the UK curriculum using British terminology and was coordinated by a 'control room' in which all guides sat in the one room and discussed students' comments and responses to particular issues. The team looking to adapt this activity for the Australian context consulted with educators and felt that the activity was too long to suit classroom programming, the scenario needed adapting. In addition, to disseminate the activity as widely as possible, the control room concept needed to be online, not in the one physical location. To enable the activity to be offered free to schools, the ACMA needed to be supported to respond to student comments and questions through the allocation of additional guides, provided by the school. Guides in the CSD activity could include ACMA staff, police and school volunteers (including teachers or parents). In addition, industry experts such as staff from Microsoft and Telstra corporations are sometimes invited to provide guides for launches to support the CSD activity.

2.2 School participation process

Schools register their interest in participating in the CSD activity by entering their details on the ACMA website, http://cybersmart.engagelive.net/ . Schools receive an automatic response to thank them for their interest, including information of the activities

[8] More information can be found at http://www.childnet-int.org/

available and details of how to schedule a time to participate in the CSD activity. On confirmation of a preferred date and time from participating schools, ACMA staff set up the activity. At least one week before the scheduled date and time for the CSD activity, ACMA staff send an email to the school with the following CSD activity resources:

- Login details for students and guides;
- A teacher's guide;
- A student's instruction booklet;
- A downloadable training module for guides;
- An online activity script; and
- Pre- and post-activity lesson plans for teachers.

On the day of the CSD activity, teachers log student teams into the portal and the game commences. Activity guides are drawn from ACMA staff, police and volunteer guides, which are provided by the school. The ACMA staff are online throughout the one hour activity managing student and guide responses and ensuring that the activity is completed successfully. In the event that a school encounters technical difficulties, ACMA staff are available by email or phone to resolve any issues (Schools are informed of the ACMA's capacity to provide technical support when the activity resources are emailed to them prior to the activity). When the activity has been completed, the ACMA staff send the school contact an email to thank them for their participation, provide a certificate for student participation and invite informal feedback.

In the format CSD has been designed, any number of schools could play on any day as they bring on resources (e.g., guides) to support student interaction. The ACMA staff team manage the administration of the game and can pull in additional resources (e.g., other ACMA staff) to assist if schools are not coping. Since its inception, there have been three revisions to the CSD script. Script writers, teachers and cyber-safety experts have been involved in these revisions to ensure the scenario is relevant and interesting to students and suited to the Australian environment, curriculum and school timetabling. Moreover, additional resources, such as Cybersmart Hero (an activity produced by the ACMA in 2010 which is focused on cyber-bullying), have been developed to engage older students in a range of cyber-safety related issues. There are also plans to launch a new activity by the end of 2011, focused on social networking, to reflect the increased use of social networking

by youth. The results and recommendations of this report will help shape the future development of the activity.

3. Methods

This section describes the methods used by the CHPRC to complete the Educational Evaluation of the CSD activity. It is important to note from the outset that the manner in which the CSD activity evaluation was conducted differed in some ways from the usual practice of the ACMA in the administration of the game in schools. The manner in which the CSD administration differed from the usual method of administration was necessary to ensure (as much as possible) that the evaluation was independently conducted and that the results were as unbiased as possible. For example, the usual ACMA administrative support provided to teachers was not always provided in this evaluation. This may have had an impact on a teacher's perception of their role within the game administration. This, in turn, could have heightened any anxiety/confusion that they may have experienced when participating in the CSD activity for the first time. These issues will be more fully explored in the discussion section below.

3.1 Stage 1: Ethical clearance

To enable the evaluation team to commence work on the formative stages of the project (all activities preceding participant recruitment and data collection) ethical declaration approval was sought and granted on 2 June, 2010. Work then commenced on a review of literature related to the evaluation of cyber-safety games and activities, social marketing and message uptake, game principles, and survey development. Full ethics approval was provided by the ECU Human Research Ethics Committee (HREC) on the 14 July, 2010 for the CHPRC to progress with the data collection and the recruitment of schools in Western Australia phase of this evaluation project. Following this approval, permission was sought from the Catholic Education Office (Western Australia) to invite schools to participate in the CSD activity evaluation. Permission was granted from this sector on 4 August, 2010. Formal approval from the Association of Independent Schools of Western Australia (AISWA) was not required but the administration office was notified of the proposed evaluation on 20 July, 2010. In the process of school recruitment, one school advised they would like both their Year 6 (students aged 11-12 years) and Year 7 (students aged 12-13 years) classes to participate in the CSD activity evaluation. As such, the ECU HREC was consulted and provided permission (24 August, 2010) to modify the ethics approval to include 13-year-old students in the CSD evaluation.

3.2 Stage 2: Interviews with the ACMA staff involved in the CSD activity development and implementation

Key ACMA staff who are involved in the CSD activity development and implementation were interviewed on the 2nd and 10th August, 2010, to provide information about the strengths, weaknesses and opportunities for improvement for the CSD activity (see Appendix 2). Interviews were conducted with five ACMA staff in August 2010; one via telephone, two via video-conference and two face-to-face. The interviews took between 20 and 45 minutes to complete and all interviews were digitally recorded with the permission of the interviewees. Information attained in this phase of the research was used to inform the data collection and analyses, as well as to enhance the research team's understanding of the strengths and limitations of the CSD activity.

3.3 Stage 3: Research evaluation and survey design framework

Due to the need for discussions with the ACMA about the functional capacity and procedures involved in administering the CSD activity in the school setting, school recruitment was somewhat delayed. As a result, the research plan was changed to conduct the student quantitative and qualitative phases in combination.

While the CHPRC recruited 12 schools to participate in the CSD evaluation, one school withdrew a few days prior to the game administration date after deciding there was too much work involved on the part of teaching staff to prepare students for the game. One school that delayed participation to Term 4 due to extended teacher illness withdrew for the same reason. Finally, one school agreed to participate before realising their Year 6 students had already participated in the CSD activity. However, the Principal at this school agreed for the teachers of these classes to be invited to participate in a telephone interview regarding their game experience. These teachers were consulted at the time of the long-term teacher follow-up (described in Stage 6) in Term 4. At this time, the CHPRC was informed that one teacher had commenced long-service leave, and the second teacher declined to participate after several attempts to schedule the telephone interview.

3.3.1 Technical difficulties

Technical difficulties were experienced at only one school during the evaluation and occurred when students were scheduled to commence playing the CSD activity. The

teacher logged on to the computers for the students, ready to play, but when the students began to operate their computers in groups of three no activity was possible. The web page was visible with the first welcome message in the inbox; however, the students could not open the message, nor could they send a message. The computers were refreshed by pressing the 'refresh/restart' button on the Internet browser window (which allowed more messages into the inbox) but interactivity was still not possible. One of the members of the CHPRC evaluation team logged out of the game and tried logging in again under 'basic mode' but found no option to choose a team number when logged back in. Two computers were able to open a message after some time had lapsed but still with no option to 'get message' or 'send message'. No student was able to send a message at any stage. As has been noted by others (e.g., Wishart et al., 2007), this is one of the potential difficulties associated with technologically-based resources.

The two CHPRC researchers visiting the school liaised with ACMA staff on the phone during the game to attempt to rectify the problems and get the game running but no solutions could be found. The ACMA suggested it may be a problem with the version of Internet Explorer at the school being Version 8:0:6001:18943 or a bandwidth problem, or possible restrictions placed on Internet Explorer by the school.

The following day the CHPRC contacted the school to arrange a time for the school's information technology (IT) person to trial logging into the game after altering a setting relating to the compatibility of Internet Explorer Version 8:0:6001:18943 with previous versions of Internet Explorer. The IT person was given instructions for how to test this during a game activity on Thursday 9th September, 2010. However no further contact was received from the IT person at this school, after three attempts to make contact with him via phone and one attempt via email (sent to the classroom teacher to forward on). In consultation with the classroom teacher, two researchers from the CHPRC visited this school to make a second attempt to play the game on Tuesday 19th October. After further technical complications and phone conversations with ACMA it was decided to restart the game. The game proceeded but towards the end of the game the computer screens started to freeze and/or automatically log teams out of the game and students thereafter could not successfully log back into the activity. Importantly, no other school experienced technical difficulties during the evaluation and this information is provided purely to provide a comprehensive overview of the evaluation process.

3.4 Stage 4: Development of national and international stakeholder group

A list of 44 stakeholders, 26 national and 18 international, with expertise in fields relating to cyber-safety was developed. In the week beginning 19 July, 2010, each stakeholder was mailed or emailed a letter of invitation to participate in a brief telephone interview discussing appropriate methods to communicate cyber-safety messages to 11 to 12-year-old students. Stakeholders who had not responded after two weeks were sent a reminder email to ascertain their interest in participating in the research. The invitation and reminder emails asked participants to accept/decline the invitation to participate.

In total, seven (two national and five international) stakeholders declined to participate; citing they were too busy, did not know enough about the game (although this stakeholder was reassured the interview would ask about cyber-safety generally, not CSD specific questions), or was on leave during the interview period. There was no response from 13 national (50%) and eight international (44%) stakeholders. Telephone interviews were conducted between late August and late October. Using the stakeholder interview protocol (see Appendix 3), a total of 16 interviews with 17 participants (nine national and eight international) were completed. One interview was completed independently and returned via email. Two others requesting this format were sent the questions via email but did not return their completed interview. This yields an overall response rate of 35% of national (*n* = 9) and 44% of international (*n* = 8) stakeholders.

Each telephone interview was digitally recorded to enable the accurate collection of data from participants. Once all interviews were completed, each digital recording was transcribed and reviewed for common themes. Due to the small number of interviews completed, one researcher (rater) reviewed all interviews. A random sample of transcribed interviews (*n* = 3) were subjectively reviewed by the researcher to identify recurring words and topologies, generating a list of common themes for each question. These common themes were thereafter consolidated into a list of content themes (codes) used to code the remaining interviews. This enabled the frequency of each theme across the full range of respondents to be determined.

3.5 Stage 5: Quantitative fieldwork with student sample

A total of 41 Western Australian Catholic and Independent schools (*n* = 20 Catholic, 21 Independent) were sent letters via fax and email inviting them to participate in the

educational evaluation of the CSD activity. All schools received a follow-up phone call and/or email to acknowledge receipt of the fax/email and were given an opportunity to ask questions regarding their schools participation in the CSD activity evaluation. One week later, schools were contacted again via email and/or phone to ascertain their participation preference. All schools received the following: a fax, an email and a phone call to see if they had any questions (some agreed to participate at this point or said they would discuss it with relevant teachers) and a follow-up phone call.

Of the 41 schools contacted for the evaluation, 18 responded to the invitation via fax, email or phone. Six schools indicated they did not want to participate in the evaluation while the remaining 12 agreed to participate. The reasons provided by three out of the six schools for declining to participate in the evaluation of the CSD activity included:

- Having no class time to allocate for students to play the game (due to the curriculum being saturated with cyber-safety initiatives);
- Already participating in Federal government cyber-safety educational initiatives (the name of these initiatives were not named or described); and
- Acknowledging the game requires a considerable amount of staff time and school resources / facilities to obtain maximum benefit from playing the game (from previous experience with a class of Year 5 students in their school).

Importantly, the schools were informed that participating in the evaluation meant data collection on two occasions and student and teacher interviews, in addition to playing the CSD activity itself. This level of commitment is significantly greater than what is usually involved in an administration of the CSD activity.

In total, 12 schools were recruited to participate in the evaluation of CSD. Of those recruited, three schools withdrew complete or partial participation. The first school withdrew partial participation due to the school contact being unaware their Year 6 students had previously played the game. However, teachers from this school agreed to participate in the teacher interview component of the evaluation. The second school, after liaising with CHPRC staff to schedule a day and time to play the game, receiving consent forms and distributing them to two classes of Year 6 and two classes of Year 7 students, registering with the ACMA and receiving login details for the game, and reading the associated CSD materials, withdrew consent to participate in the evaluation. This school did so due to feeling

their school staff were not appropriately trained to confidently act as guides during the game play and were uncertain of the guide roles and/or responsibilities for the day. After postponing participation to Term 4, one further school withdrew due to long-term teacher illness. Finally, 23 schools did not respond to the letter of invitation or follow up phone call/emails. Further contact was not made with these 23 schools as the recruitment deadline for the game and evaluations to occur in Term 3 had passed.

Data collection with students and teachers commenced on Thursday 2 September, 2010; when nine schools completed the evaluation components and played the CSD activity (see Data Collection Schedule – Appendix 4). In these nine schools, 13 classes with a total of 341 students were scheduled to play the game and participate in the pre- and post-CSD survey in Term 3 (between the 2nd and 17th September, 2010). Overall, 292 students (from a possible 329; 89% response rate) completed the pre-test survey. Forty-nine students did not complete the survey due to being absent on the day of game administration and parental consent was not obtained for 12 students. This resulted in an overall response rate of 89% response rate. Most (269 out of 292; 92%) students completed the post-game survey, with 87 students (42 boys and 45 girls) participating in eighteen focus groups. The post-test surveys were administered 1-2 weeks after exposure to the CSD activity.

Once a school was recruited (permission was provided by the School Principal or Deputy Principal), contact with the school continued with the classroom teacher. Due to the large amount of time this staff member spent in the classroom with students, it was often difficult to re-establish contact to confirm specific details pertaining to game activities. Six schools scheduled and played the game without any difficulties, while three schools required rescheduling to different times or days due to clashes with ACMA commitments.

Prior to participating in the CSD activity evaluation, parent consent was required. The ECU HREC and Catholic Education Office granted permission for the use of active/passive consent. This means that parents were first sent a letter of information about the evaluation and asked to return a form indicating if they did/did not want their son/daughter to participate in the evaluation (active consent). The consent form sought parental/carer permission for their child to participate in the game, complete the pre- and post-test survey and/or the focus group. A week later, a second letter was sent home to parents of students in participating classes advising them if they do not want their son/daughter to participate in CSD activity evaluation they must return the consent form

indicating this (i.e., noting their lack of consent for their son/daughter to participate in the project), otherwise their son/daughter would be provided with the questionnaire and invited to play the CSD activity (passive consent).

Year 6/7 teachers or coordinators from all 10 schools recruited to play the game were posted parent (active: Appendix 5a; and passive: Appendix 5b) information letters (describing the project) and consent forms. Teachers were asked to distribute one information letter and consent form to each student in their class. Once signed by the parent/carer, the consent form was to be returned to the class teacher for safekeeping. Each teacher was provided with a secure envelope to store signed and returned consent forms. Consent forms were collected by the CHPRC team upon visiting each school to administer the pre-test survey and post-game focus group. Only students with parental consent were included in the game surveys and focus groups.

Two evaluation team staff visited each school on the day that students played the CSD activity. Immediately prior to game commencement, students for whom parental consent was provided completed a short written questionnaire about their Internet and mobile phone use behaviours, and experiences with others (people known and unknown to them) while using technology (Appendix 6). The questionnaire was coded with an identification number to enable linking the student's pre- and post-game surveys. The questionnaire took approximately 20 minutes for students to complete and was then collected by the CHPRC researcher. Students then played the CSD activity. The researchers were advised by the classroom teacher where they should wait while the students were engaged in the game activity. At some schools, the researcher waited outside the room while students were playing and at others they waited in the room. At each school, the researcher advised the classroom teacher that their role was to observe the game, not interact with students.

Maintaining an independent role in the administration of the game and the feedback to students and/or guides during the game was essential to ensuring that the data collected is as unbiased as possible. In all administrations, the goal was to ensure that the CSD activity administration as closely approximated the normal administration of the game as possible (i.e., in those schools that are not involved in the evaluation project). This means that the CHPRC staff, at all times where possible, worked to minimise the level and nature of contact with students and/or guides in relation to the game content, instructions and aims.

However, it is recognised that the type and level of contact that the ACMA staff usually has with schools during the CSD set-up and administration differs from what the schools in this study experienced, and direct communication between the school and the ACMA can impact the student experience by providing feedback to resolve technical or other issues. This feedback (especially during the implementation of the game) needed to be provided by the ACMA team in the usual way. Outside of the evaluation, if a nominated guide was not interacting with students online, the ACMA would contact the guide and discuss the process of responding with him/her. As evaluation school's identity was kept anonymous, the ACMA were able to phone one of the researchers visiting the class to conduct evaluation activities. In the event that the ACMA phoned the researcher, the phone was passed to the guide to enable the usual process of guide instruction to proceed.

Following the game activity, the teacher was asked to randomly select six male and six female students to participate in a focus group discussion about the CSD activity. The researcher ensured each student had consent to participate in the focus group (parents were asked to provide consent for their son/daughter to complete the questionnaire and/or participate in the focus group) before proceeding to follow the focus group protocol in a room nearby the students' classroom. At the conclusion of the focus group, the researcher thanked the students and classroom teacher for their assistance and time that day, confirmed the date and time to return for the follow-up survey and left the school taking all completed consent forms, questionnaires and focus group digital recordings to be stored securely at ECU.

3.6 Stage 6: Qualitative fieldwork with student and teacher sample

3.6.1 Student focus groups

The qualitative fieldwork stage was conducted concurrently with the quantitative fieldwork stage (Stage 5) in August/September 2010. Immediately following participation in the CSD activity, a selection of students participated in a focus group discussion to elicit detailed information about students' perceptions of the activity. In each school, a minimum of two focus groups were conducted; one with female students and one with male students. Splitting the focus groups by gender enabled students, especially girls, to provide feedback about the CSD activity more freely and the segmentation permitted similar participants to be partnered together, resulting in diversity across groups rather than within groups [79]. This homogeneity enhanced the group dynamic and resulted in participants feeling less inclined to spend time justifying responses. Moreover, it facilitated quality discussion by allowing

more time to discuss priority issues. As discussed in Stage 5 above, eighteen focus groups were conducted at nine schools. One school was an all girls school and thus two focus groups were conducted each comprising six girls. Moreover, due to high numbers of absenteeism on the day of the assessment at one school, it was necessary to conduct two focus groups comprised of both boys and girls.

Each focus group was digitally recorded to enable the accurate collection of data from participants and allow for each to be transcribed. A random sample of transcribed focus groups (n = 6) were subjectively reviewed by three researchers to examine themes related to barriers and enablers for key message identification and assimilation as well as suggestions for the future development and enhancement of the CSD activity. These three researchers then independently allocated content themes (codes) for each main question asked in the focus group. Two of the three researchers and one moderator then met to discuss the individually identified themes to generate final content themes for each question. Two raters were used to identify/generate the common themes but one rater then used those themes to code the focus group transcripts. All remaining focus group transcripts thereafter were coded using the final set of content themes (codes), allowing for the frequency of each theme across all focus groups to be determined.

3.6.2 Teacher interviews

The classroom teacher was invited to participate in a brief (10 minute) interview approximately one to two weeks after their class participated in the CSD activity. The aim of this interview was to understand the organisational requirements involved in planning the administration of the CSD activity, staff perceptions on the pre/post game resources associated with the game and thoughts relating to message uptake and retention by students. The interview took place on the same day and time as the post-game questionnaire scheduled with students. A total of twelve face-to-face interviews were successfully completed with teachers from nine schools participating in the short-term evaluation.

A further eight teachers (who had previously completed the CSD activity with their students) who registered an interest with the ACMA regarding the CSD evaluation were contacted by the CHPRC staff and invited to participate in the long-term CSD follow-up. Six out of the eight teachers who agreed to participate completed an interview. One teacher

could not participate as they were on long service leave, while the other declined to participate.

Eleven out of the twelve short-term and all the long-term teacher interviews were digitally recorded (one short-term evaluation teacher did not consent for the interview to be recorded) to enable the accurate collection of data from participants. Once all interviews were completed, each digital recording was transcribed and reviewed for common themes. A random sample of transcribed short-term (*n* = 3) and long-term (*n* = 3) evaluation interviews were subjectively reviewed by two researchers to identify recurring words and topologies to generate a list of common themes for each interview question. These two researchers and one moderator then consolidated the individually identified themes into two content theme (codes) lists for each interview type (i.e., one for short-term and another for long-term) and were used to code all remaining interview transcripts. As above, two raters were used to identify/generate the common themes but one rater then used those themes to code the focus group transcripts. This enabled the frequency of each theme across the full range of respondents to be determined.

3.6.3 CSD activity transcripts

The ACMA provided a Microsoft Excel file comprising data downloaded from all CSD activity administrations (i.e., nationwide) completed during the evaluation period. The files contain a list of questions posed by students, and responses provided by guides, during a CSD activity. Data was provided to the CHPRC in this format for all 46 CSD activity sessions held during the evaluation data collection period (June to October 2010). From these data, the CHPRC reviewed each transcript to determine the nature of the questions/comments students posed during game play. In addition, the CHPRC grouped guides' responses to students' questions/comments in each game activity. This grouping enabled content analysis of guide responses according to the type of guide providing the response (e.g., ACMA staff, volunteer, or police).

3.7 Stage 7: Interviews with national and international stakeholder group

Details of interviews conducted with national and international stakeholders are provided in the section describing Stage 2 of this evaluation.

4. Results

4.1 ACMA staff interviews

In interviews conducted prior to the commencement of the data collection phases with stakeholders, teachers and students, ACMA staff identified a number of known strengths and limitations of the CSD activity. These points are described here to provide a context for the results arising from the data collection.

4.1.1 CSD activity strengths

ACMA staff reported that the main strength of the CSD activity was to provide a collaborative, engaging and fun learning environment. In addition, the simple and realistic scenario ensures relevance with the student audience and the interactive format enables open communication channels. The ACMA staff believe that the activity is seen as a credible source of cyber-safety education. The staff also reported that, the involvement of police as guides during the activity adds value. In the ACMA's experience, students respond positively to the interaction with police and value them as a credible source of cyber-safety advice.

4.1.2 CSD activity limitations

Some limitations exist that may hinder the impact of the CSD activity. The ACMA staff interviewed identified several weaknesses (e.g., the ability to follow a string of messages for a team; that it is a fixed script; it's a one time only activity; some resources must be provided by schools; and school Internet security settings and broadband access can have an impact on the schools experience during an activity), some of which are currently being addressed. In addition, other suggestions may offer opportunities for improving the game and its administration. Differences between each state's education system, and between the educational sectors (i.e., Government, Catholic, Independent) can provide challenges as cyber-safety is included in different parts of the curriculum. Therefore, it can be difficult to know who to contact to advertise the game and promote school's participation in it. Similarly, identifying the ACMA's role in cyber-safety education and how to

promote this to schools can present challenges which impact on the level of awareness and adoption of the CSD activity in the school environment.

In terms of administering the activity, school Internet speeds and available bandwidth are a key limitation in a school's capacity to participate in the activity. The technological literacy of guides provided by the schools can also influence the level of interactivity and the appropriateness of the responses provided to students. Relying on schools to provide guides can be problematic as there is no guarantee the required number of guides will be found, nor be available on the day of the activity. If the school is unable to provide a sufficient number of guides, it falls to the ACMA to meet any shortfalls. Moreover, the ACMA have no current mechanism to identify if teachers and students engage in pre- or post-game activities, which are developed to enhance students' understanding from the game. Furthermore, there is currently nothing in place to determine if students apply what they have learnt to real life situations outside of the game scenario although this would be difficult to achieve. Finally, the text-based format of the game and the speed with which messages are sent to students (which can move somewhat quickly) may prove difficult for students with lower literacy levels, attention or other types of learning difficulties. Importantly, these factors were not measured as part of this evaluation so it is unknown if they had an impact on the results.

This section presents the results of each stage of this process evaluation. First, themes arising from telephone interviews with key stakeholders in the field of cyber-safety are presented, followed by a discussion of responses provided by teachers regarding their perceptions of the CSD activity. The next section presents results from the quantitative surveys completed by students before and after participation in the CSD activity, followed by discussion of themes arising from student focus groups.

4.2 Stakeholder interviews

Stakeholder interviews were conducted between 7 August and 7 October 2010. Each stakeholder interview took between 15 and 45 minutes to complete. Sixteen interviews were completed with 17 participants; one interview comprised two participants. The majority of participants were female (71%) from a variety of age groups above 30 years (Table 1). Most participants had a post-graduate level education (Bachelor Degree = 29%, Post-

Graduate Diploma or Masters = 47%, Ph.D. = 24%). Slightly more national (53%) than international (47%) participants completed the interview.

Stakeholders who participated in this stage of the evaluation represented organisations that focus on Internet safety education, Internet protection software, Internet and computer service providers, cyber-crime experts, cyber-safety research and cyber-safety awareness-raising in the community. The majority of the stakeholders interviewed were not familiar with the CSD activity.

Table 1. Demographic characteristics of national and international stakeholder group

Characteristic	Response	%	Total *(n = 17)*
Gender	Male	29	5
	Female	71	12
Age	30-39 years	30	5
	40-49 years	35	6
	50 years or older	35	6
Qualification	Bachelor degree	29	5
	Postgrad / Masters	47	8
	PhD	24	4
Location	National	53	9
	International	47	8

Stakeholders were asked to comment on the strategies they felt were necessary for schools to address cyber-safety (Table 2). Stakeholders reported strategies for schools to address cyber-safety would likely include: policy development or review, parent involvement, professional development for school staff in using new technologies, promoting a respectful and caring school community and cyber-safety curriculum materials for students. Most stakeholders also reported they would include: establishment of a whole-school committee, encouragement of teachers to model the safe use of technology and local community involvement. Some would also include an interactive online game for students, online advertising/promotion about cyber-safety and Internet filtering products. Two stakeholders suggested a lead role for students/student voice. The following strategies were reported by

one stakeholder each as important components of cyber-safety programs: prevention/detection reporting and intervention, reporting structure and grading of offences.

Table 2. Recommended components of cyber-safety strategies

Theme	Total *(n = 17)*
Parent involvement	14
Policy development or review	14
Professional development for school staff in using new technologies	13
Cyber-safety curriculum materials	12
Promoting a respectful and caring school community	12
Encouraging teachers to model the safe use of technology	11
Establish a whole school committee	11
Local community involvement	11
Interactive, online game for students	10
Online advertising about cyber-safety	9
Internet filtering products	7

4.2.1 Format for cyber-safety educational activity

Stakeholders were asked about the format they would recommend for delivering a new technology-based cyber-safety educational activity for 11-12-year-old students; with the majority of participants reporting this would be in an online format as this is the most relevant and appealing format for students of this age. Many reported that it should be embedded in-the curriculum and some would also use pamphlets, books and other printed material to support activity delivery. Four stakeholders reported peer-to-peer education would be a format they would use to deliver a cyber-safety educational activity. Three stakeholders reported the online activity should take the form of an online game, *"a game speaks to them in a way that an adult cannot",* and three, that the online activity should be created by students. While stakeholders interviewed did not expand on how this process might operate in a school setting, students who participated in the focus groups offered some suggestions in a related fashion.

Stakeholders were asked specifically about the usefulness of an interactive online game to communicate cyber-safety messages to this age group (Table 3). Eight reported

that an online game would be very useful to communicate cyber-safety messages to this age group as it would be appealing to students, four thought it would be useful, three somewhat useful and one reported that an online game would not be useful due to their belief that games are not effective in creating behaviour change.

Table 3. Stakeholders' perceptions on the usefulness of an online interactive game to communicate cyber-safety messages to this age group

Theme	Number of respondents *(n = 17)*
Very useful	8
Useful	4
Somewhat useful	3
Not useful	1

NB: one stakeholder did not choose a particular category

Two of the interviewees commented a game would need to reinforce positive messages and can't just be stand-alone, therefore would need to be supported by ongoing education and promotion.

Participants were asked how they, or their organisation, would promote a cyber-safety game to schools. The majority of participants reported that they would offer teacher professional learning and involve education sectors to communicate and promote their game to schools. In addition, several stakeholders reported a website would be a useful source of information for schools. Mail out, peer messaging (i.e. *"using older students such as 14 year olds to convey the message including real stories"*) and promotion based on the social marketing advice of their and other organisations were also identified by stakeholders as methods of promotion. Four participants didn't answer the question although some of these offered comment:

> *"Up to the whole of school committee: teachers, P & C and student committee, to determine how a cyber-safety game would be promoted."*
>
> *"My organisation does not do such promotions."*

"Partner with 'gamers' (i.e., people who create games) to develop and disseminate the game as that is their profession and there is no point in reinventing the wheel."

"Partner with Lego or something that is a tangible product and have kids interacting… work on a game that has levels and rewards e.g. a Lego prize or AFL items."

When asked in what ways their organisation would support schools in implementing a cyber-safety resource, such as a game for 11-12-year-old students, five stakeholders reported that they would provide media/website promotion. Demonstrating the varied nature of the organisations represented in the stakeholder consultation phase of this evaluation, an array of other support roles included: teacher professional learning, newsletters, educational resources, presentations and technical help, data collection to assess effectiveness and provision of reward based promotional resources. Four participants reported that support for schools in implementing a cyber-safety resource was not the sort of work their organisation would be engaged in.

4.2.2 Cyber-safety messages for 11-12-year-old students

When asked their perception on the most important cyber-safety messages to communicate to 11-12-year-olds (Table 4) one stakeholder replied *"it's hard to boil it down to a few words because we're at a stage today where there's so much to teach them".*

An overwhelming majority of stakeholders reported personal responsibility for cyber-safety as the key message to communicate to this age group. Many cited respectful behaviour and the permanency of their digital footprint. A few participants reported 11-12-year-old students should be taught what is inappropriate content, contact and conduct.

When asked about the most effective strategies available to communicate cyber-safety messages to 11-12-year-olds, a large number of respondents mentioned using visual techniques and increasing opportunities for learning about cyber-safety in the classroom. In addition to these strategies peer-to-peer activities, embedding cyber-safety in the curriculum, message repetition and case studies were suggested.

Table 4. Most important cyber-safety messages to communicate to 11-12-year-olds

Cyber-safety message	Total *(n = 17)*
Personal responsibility for cyber-safety	16
Respectful behaviour	7
Permanency of their digital footprint	5
What is inappropriate contact	4
What is inappropriate conduct	2
What is inappropriate content	2

NB: Respondents could have identified more than one theme.

4.2.3 Critical success factors and barriers for the effectiveness of cyber-safety games

The most commonly listed factors stakeholders reported would enhance the success of a cyber-safety game included: the need for it to be current and relevant, fun, engaging and focused on positive messages. Other factors suggested to enhance the game's success were that it could include rewards and goals, be visually appealing to students, competitive, multi-player and easy to use.

When asked about barriers affecting the game's success, stakeholders suggested should a game be boring, irrelevant or not technologically appropriate it would not succeed. In addition, it was mentioned by three stakeholders that the success of a game would be hindered if its concept was misleading:

> *"If a game doesn't meet kids expectations such as if it doesn't do the right things, use the right keys etc. then success would be limited."*

One participant suggested avoiding the use of educators in favour for gamers:

> *If they [students] perceive it as something about safety they may not want to play. If it's old fashioned, they won't want to do it. Create the equivalent of online games they are playing now. You may not want to call it a game as they will expect certain things about a game."*

One stakeholder suggested it would be best to avoid using adults to develop things they think students need to know. Students need to be involved in the development and review of a game:

> *"A game has got very limited educational possibilities. As soon as you make it educational, it loses the point of being a game."*

When asked about the barriers to schools' implementation of a cyber-safety game, stakeholders reported lack of technology and teacher resources as the largest barriers. In addition, stakeholders felt the value of the game perceived by the school/teacher/parent and their willingness to adopt it could be a barrier to implementation. Lack of time, the effectiveness of the game, competing agendas/priorities, lack of awareness of the product and cost were all mentioned as possible barriers to implementation.

4.2.4 Advantages and disadvantages of online games

Stakeholders were asked their thoughts on the advantages and disadvantages of online games. A large majority of respondents reported the ease of access to be the most important advantage of online games. Other advantages included: appealing to students, cost-effective to deliver, promotion of positive use of technology and inexpensive for schools. The advantages of online games are represented by the following commentary:

> *"It is an up to date, global form of engagement that the young are used to dealing with."*

> *"They do so much informal learning through media and technology."*

Numerous disadvantages were suggested including: reliance on the Internet which may at times be slow, unavailable or subject to power failure, questionable security/accuracy of information online, competition with other online resources (e.g., how to know which are effective) and access to technological resources (e.g., computers in schools).

In addition, cost, compatibility issues (such as having the latest software, Internet speed and hard drive size required), different learning styles of students, reliance on an external service provider and time involved in organising the activity were all cited as possible disadvantages of online games. Cyber-safety message saturation was suggested as an additional disadvantage:

> *"the online resource world creates so much noise nobody can hear anymore".*

4.2.5 Summary

In summary, stakeholders who participated in the interviews represented a wide range of organisations that focus on aspects of cyber-safety ranging from education and research to service providers and cyber-crime experts both nationally and internationally.

Numerous promising strategies to address cyber-safety were recommended including policy development and allowing students to take a lead role and have a voice in addressing cyber-safety. An online format for cyber-safety educational activities was supported by the majority of stakeholders, with online games being suggested as a very useful means to communicate cyber-safety messages to 11 and 12-year-old students. It was suggested by most stakeholders that online games can be effective as they are both appealing and relevant to the target audience.

Stakeholders reported that the promotion of a cyber-safety game to schools could be done through teacher professional learning and development. This could involve all education sectors to best promote the game and advertise the games objectives and key outcomes. Promoting the evidence-based nature of the game is an important element of communicating the effectiveness of this approach to cyber-safety especially given the dearth of resources that have been subjected to critical and empirical analysis. Furthermore, personal responsibility for cyber-safety was reported as the key cyber-safety message to be communicated to 11 and 12-year-old students. This can be somewhat challenging and due consideration needs to be given to the developmental experiences of the target group as well as the general level of functioning (cognitive, emotional, social, psychological, and technical) of this age group.

Critical factors for the success of cyber-safety games included the need for it to be current, relevant, fun, engaging and focus on positive messages. Suggested barriers to success included: should the game be boring, irrelevant, not technologically appropriate, or did not include components expected by youth to be included in a game. Lack of technological and teacher resources were cited as the main barriers to school's implementation of a cyber-safety game. Easy and instant access was reported as the most important advantage of online games, whilst reliance on the Internet was seen as a disadvantage.

4.3 Teacher interviews

The following presents a summary of teacher responses to in-depth interview questions asked as part of a one-on-one interview regarding the evaluation of CSD. Interview respondents included teachers from schools recruited by research staff at the CHPRC to participate in the evaluation (short-term evaluation) and schools who had previously contacted the ACMA to play the CSD activity (long-term evaluation). In this section, major themes are highlighted in bold text and the summary of responses is grouped by evaluation school type (i.e., short-term or long-term).

A total of twelve face-to-face interviews were successfully completed with teachers from nine schools participating in the short-term evaluation. Interviews were completed between seven and 14 days after each class had played the CSD activity at a day and time that best suited the class schedule. The time period between the pre and post-test sessions was primarily determined by the school schedule and when the evaluation team could best be accommodated on two testing occasions. A further eight teachers who registered an interest with the ACMA regarding the CSD activity evaluation were contacted by the CHPRC research staff and invited to participate in the long-term follow-up. Six out of the eight teachers who agreed to participate completed an interview. Of these teachers, only one had played the game in 2010 (this year), while the majority played the game in 2009 (last year). Two long-term evaluation teachers reported playing CSD more than once, with teachers playing up to three years ago.

The main themes have been written as a qualitative summary and are discussed in text using the terms ‘majority’, ‘most’, ‘many’, ‘some’ and ‘a few’. Each of these categories are based on the number of references and sources of information following the thematic coding process. Supporting quotes (both positive and negative) are presented with the school pseudonym (school ID) and evaluation type (ST= short-term, LT= long-term) to highlight CSD activity strengths and suggestions for improvement. For example, “Scl_012_ST” would refer to a teacher from school number 12 who participated in the CSD activity recently (i.e., in the previous six months). In contrast, “LT_B” refers to a teacher from school B who participated in the CSD game at least 12 months previously.

Three-quarters of the short-term participants (*n* = 9) and almost all long-term participants (*n* = 5) were female. The majority of short-term participants were aged between

25 and 34 years (Table 5) and had between six and ten years of teaching experience (Table 6). The ages of long-term participants were more varied, ranging from 25 to 60 years (Table 5) with teaching experience ranging from six to more than 26 years (Table 6). In total, twice as many participants had completed a Bachelor degree (*n* = 12) versus a Post-graduate or Masters qualification (*n* = 6).

Table 5. Age of short and long-term evaluation teachers

Age group	Short-term (*n* = 12)	Long-term (*n* = 6)	Total (*n* = 18)
25-29	4	1	5
30-34	3	0	3
35-39	2	2	4
40-44	0	1	1
45-49	1	0	1
50-54	1	1	2
55-59	1	0	1
60 +	0	1	1

Table 6. Years of teaching experience

Years of teaching experience	Short-term (*n* = 12)	Long-term (*n* = 6)	Total (*n* = 18)
0	2	0	2
1-5	3	0	3
6-10	4	2	6
11-15	0	2	2
21-25	1	1	2
26+	2	1	3

4.3.1 CSD activity impressions

Respondents were initially asked to describe what they could recall about the CSD activity. The majority of short-term and some long-term evaluation teachers could recall details pertaining to the **game scenario and content** (i.e., the story within the game) or the process their students undertook in order to play the game (**student involvement**):

> *"A telephone had been found in the playground and I think the mobile phone was asking the person who found it, who they are. From that they were trying to figure out who the mobile phone belonged to and they suspected it was someone from school; and then they realised the person from their school was not there that day. As the student was absent, they thought it was a little bit fishy as to where she was. Then the students looked at some messages on the phone and they then thought she had been contacted by someone she didn't know and was going to meet them."*
>
> [Scl_012_ST]

> *"The students had messages coming in and then they had to reply to these and then usually someone would reply to their message."* [Scl_012_ST]

However, the majority of long-term evaluation teachers made reference to **student responses**, specifically recalling how much they engaged with the game:

> *"The characters were really quirky and interesting for the students. The messages were great and it seemingly was entertaining and involved the students."* [LT_B]

Some short-term evaluation teachers commented on the process of preparing for the game and managing their role as a guide (**game process**). Specifically, commentary suggested short-term evaluation teachers were initially **confused** as to their role during game play and found it very **difficult to source another guide** to assist during game play:

> *"It was not possible for us to provide two guides. We would have to combine two classes and ask for parental help or link it with computer time so [the computer teacher] was in the classroom also."* [Scl_007_ST]

> *"Trying to find a guide really places pressure on schools. The only way we could manage was to recruit one of the prac[ticum] teachers to be a guide. Trying to find a spare teacher is really not that easy."* [Scl_001_ST]

Consequently, short-term evaluation teachers were predominantly the only guide provided by each school and therefore some reported that they found it **difficult to simultaneously manage** student responses and monitor classroom behaviour[9]. One teacher commented that

"it would be better if [the] ACMA could provide more guides so that each school participating in the game receives consistent support and messages. Cyber-safety is their [the ACMA] expertise, so they know the best way to respond [to student questions]." [Scl_005_ST]

Respondents also commented on their **preference for monitoring student behaviour** and **assisting students face-to-face** rather than interacting as an online guide:

> *"It would have been better if we could assist the students [face-to-face] as they answer the questions."* [Scl_007_ST]

One respondent indicated they found it difficult to not only keep up with student questions, but to also **keep track of responses provided to the various teams in order to streamline information** and ensure all questions sent to them by students were answered:

> *"It was difficult to keep track of what you'd said to each team – 'what did I say to who?'"* [Scl_004_ST]

> *"When we were in the control room as guides, both of us felt the messages coming through from the children needed to stay up longer. They [messages] tended to drop off the screen quickly, so that by the time we got back [following responding to another message], it had disappeared and we couldn't answer them. So we would like to see messages stay up longer to give us more time to respond. The other thing was…we can get a message from them [students], but we don't know what they are referring to. Sometimes we have five teams all sending email and it becomes very difficult [to know what each is asking and respond to them all]."* [Scl_005_ST]

One respondent reported that the thought of being a control guide created feelings of **anxiety** as they were not confident in their cyber-safety knowledge or their ability to effectively participate as a control guide:

[9] This may be an artefact of the methodology employed as part of this evaluation and may be inconsistent with the standard administration.

"I would have felt more confident if they [the ACMA] had participated more [during the game], so we could hang back a bit more to allow them to use their expertise. It can be quite stressful when they [students] are trying to send you messages – you think to yourself 'oh, what am I saying… am I saying the right thing… who said what?'"

[Scl_005_ST]

Conversely, another respondent commented they were excited with the prospect of being a guide and found the experience very **enjoyable**:

"I really enjoyed being a guide and really embraced the challenge." [Scl_004_ST]

The majority of long-term teachers were **somewhat comfortable** with their role as a guide during the CSD activity as *"you're certainly on your toes during the game"*. Some indicated, as teachers, they have to be able to effectively communicate with their students. Responding to student's questions was, therefore, second nature:

"[Playing the game enables you to] find out things about your children that you might not have been aware of before." [LT_A]

"It's one of things primary school teachers [have to do]… [teachers are] a jack of all trades and a master of none." [LT_B]

However, a few long-term evaluation teachers indicated they were **uncomfortable** with their role as they found being a guide very **challenging**, indicating they would have valued **more guidance** in preparing for the game and support as an online guide:

"I felt insecure and would have loved an outsider to be with me at school [during the game]." [LT_C]

"I found being a guide particularly challenging as it was difficult to know what to say [in response to students' questions]." [LT_D]

Consequently, one long-term evaluation teacher indicated they would have valued the opportunity to utilise a professional **external guide**:

"I really needed more guidance and would have liked to book someone to give outside influence." [LT_C]

Approximately half of the long-term evaluation teachers indicated the optimal number of students to allocate per team would be **three**. It was suggested that this number of students allows for greater opportunities to discuss questions and appropriately resolve the CSD activity scenario. However, the difficulties in allocating an appropriate amount of space between each teams' computer was noted. Consequently, some short- and long-term evaluation teachers suggested that **two** students per team would be optimal:

> *"I think it would be better if there were two students per group just to fit around the computer, but three worked."* [Scl_010_ST]

One long-term evaluation teacher commented that students should work through the game **individually** as *"at that age… that's the real world when they are on a computer … [working in a group] influences their responses."* [LT_C]

4.3.2 Cyber-safety awareness

Respondents were also asked to identify what they understood to be the key messages promoted in the game. The majority of short-term evaluation teachers indicated the game encouraged users to be *"streetwise"* and **not communicate with people online you don't know face-to-face.** Many short-term and a few long-term evaluation teachers also noted the game prompted students to **not meet people face-to-face you only know online**:

> *"Don't get involved with anyone online you don't know [face-to-face]."* [Scl_004_ST]

A few short and long-term evaluation teachers also suggested the game highlighted how easy **it is easy for others to conceal their identity online**, indicating students should **only have online friends they also know face-to-face**:

> *"Being aware of the fact that people aren't what they seem to be online, and can create virtual personalities."* [Scl_001_ST]

The majority of long-term evaluation teachers suggested the game encouraged students to be responsible for their own actions, indicating youth should be aware of their **digital responsibility**:

> *"On the Internet it's an open world and they have responsibility for their own actions."* [LT_C]

Some short-term evaluation teachers also noted the game encouraged students to **seek advice from friends, parents and/or police when necessary** as a means to safely resolve issues or **set their social networking profile page to private**:

"Ask an adult when you get into difficulty." [Scl_005_ST]

"If you were to get involved [with someone you don't know] tell someone about it who can do something about it. The best message is to not get involved at all."

[Scl_004_ST]

A few short- and long-term evaluation teachers also indicated the game encourages users to **limit/remove or to not post personal information published online**; with long-term evaluation teachers further commenting the game encouraged students to consider their **digital footprint**:

"Anything you put online stays online… never give away personal information like your home address… need to take responsibility for anything that you do post. If you didn't want your grandma to see it, you wouldn't want your friend to see it."

[LT_B]

The majority of short and long-term term evaluation teachers indicated these aforementioned cyber-safety messages were **very appropriate** or **appropriate** for students aged 11-12 years old, identifying **there is a need** for cyber-safety activities as **technology is part of their everyday life**:

"That type of technology, be it the net, emails, MSN, etc… is part of their life these days. So they have to be aware of what's going on." [Scl_004_ST]

The majority of short-term and a few long-term evaluation teachers also commented that the messages contained within the game **increases knowledge and understanding** of cyber-safety and the potential risks of communicating via online technologies:

"Well, it's astounding to me how many students, who I thought knew about this, just don't." [Scl_001_ST]

"Kids are using technology at a younger and younger age so they need to be made aware of problems that the Internet poses or that mobile phones have."

[Scl_006_ST]

Further, short-term teachers commented the game proved to "**reinforce** what we teach about Internet safety in the classroom" [Scl_005_ST] and highlights to students why online rules and restrictions are in place:

> *"It's great for them [students] to see why their parents choose to restrict or limit their Internet access"* [Scl_001_ST]
>
> *"They've all got mobile phones and they are all using the Internet. I think they are aware of the messages, I am just not quite sure they carry it through"*
>
> [Scl_010_ST]

A few short- and long-term teachers also commented the game would be more user-friendly if there was an option to **choose from a range of scenarios based on individual school needs**. For example, one teacher commented that *"cyber bullying is something that can and has occurred and is something I would like to target"* [Scl_007_ST]. Another teacher suggested they would like to make the game *"part [of] a whole school program with different scenarios throughout the year"* [Scl_006_ST].

Interestingly, some short- and long-term teachers also had concerns regarding students utilising their newfound cyber-safety knowledge outside the game environment, suggesting it **was only a game and therefore may not be translated into practice**:

> *"They know it was a game and I don't know how seriously they took it"* [Scl_007_ST]
>
> *"I was surprised with how quick some of the children were to pick up on the messages in the game and follow the scenarios – but I am not convinced… especially students in this class, as they are prone to giving out personal information. Because they know it was a game – I don't think they could see the seriousness of it."* [Scl_012_ST]
>
> *"[The game] doesn't actually change the way students behave… students don't take it seriously. They know and give the right answers but don't put it into practice."*
>
> [LT_E]

4.3.3 Preparing to play the CSD activity

The majority of long-term teachers heard about the CSD activity through their education sector administration via newsletters, mail and/or email. Further, two long-term teachers reported discovering the CSD activity after conducting an Internet (Google) search for cyber-safety information. Long-term teachers indicated they utilised the CSD activity in their class **as part of a suite of cyber-safety activities**, with only one teacher playing the game as a **one-off event**.

Almost all short-term and a few long-term evaluation teachers indicated they spent **no more than 30 minutes** organising the CSD activities. The remaining long-term teachers spent **between one and two hours**, with one teacher **unsure** of the length of time spent preparing for the game. All evaluation teachers were either **very satisfied** or **satisfied** with this amount of preparatory time. Respondents indicated they utilised this time to scan through the CSD materials and brief their class on the game topic and purpose.

Further, short- and long-term evaluation teachers **did not source any other information or resources** to assist them organise the activity, commenting they only utilised the ACMA CSD activity materials[10]. However, many short-term evaluation teachers admitted they neglected to read through the CSD preparatory information as they were overwhelmed with the amount of content (**too much information**) or had **competing priorities**. A few short-term and one long-term evaluation teacher indicated they were time poor (**lack of class time to fully prepare**) and could therefore not read through the CSD materials provided:

> *"Getting ready for the game wasn't such an issue, it was reading through the material that I found quite difficult…it was somewhat obscure... and as a teacher at this time of year we've got a fair bit of work on."* [Scl_006_ST]

> *"There was quite a lot of information to read and I must admit, I only skimmed through the content – so I was a little 'Oh, I will be fine' as I thought all the information was there to read only if you wanted to know more about what your students will be doing. I didn't see anything that said, your responsibility will be this... so, that needs to be a bit clearer - might have just been me though [laughing]."* [Scl_010_ST]

[10] These will be added as Appendices in the final report

"I did not go through all the information because there was just so much of it. There was just too much information, because just time wise and everything else that goes on in schools, there is not enough time to sit down and read the manuals or even play the game yourself." [Scl_001_ST]

Due to the aforementioned difficulties, one short-term respondent indicated they were **not satisfied** with the amount of time required to organise the CSD activities for their class. As a means to alleviate the aforementioned difficulties, a few teachers commented they would value **a succinct overview of the game requirements**:

"Being a teacher, we're really, really busy and we have six other subjects to organise so we need things in a really simple step by step manner. The documents were really informative, but there was a lot of repeated information in every single one, so you could almost have a teacher guide on one page – taking out everything else and only including what exactly we have to do…even getting a teacher to write it, because teachers know we just don't have the time." [Scl_008_ST]

Notably, a few short-term evaluation teachers had **previous experience playing the CSD activity** and therefore did not read through the materials provided due to feeling confident of the requirements and process involved in playing the game.

4.3.4 Pre & post game activities

Four out of the six long-term evaluation teachers did not complete the pre-game activities while almost all (ten out of the 12) short-term teachers **did not complete either the pre or post CSD activities**. Those teachers who did complete **some** of the pre-game activities indicated they either **made modifications to reduce their length** or **limited activities to a class discussion**:

"To create more of a discussion to find out what's happening at home on the Internet." [LT_C]

Two long-term evaluation teachers indicated they completed all the pre-CSD activities with their class. One of these teachers **could not recall** any detail of the activities while the other remembered their students were engaged with the activity. This teacher

further suggested the pre-game activity **enabled discussion to be directed toward finding out about student's online interactions**. These two long-term evaluation teachers also commented the pre-game activity provides teachers with **good guidelines for those unfamiliar with cyber-safety** and **increases one's understanding of the topic**:

> *"[The pre-game materials] gave the teachers a chance to gain an understanding of what it [the CSD activity] was about"* [LT_A]

The only comment made with regards to what teachers disliked about the CSD activity pre-game activity was a **lack of detail**. Specifically teachers suggested the CSD activity materials (inclusive of the pre-game activities) required a more teacher friendly approach; a feeling echoed by short-term evaluation teachers in their desire for a succinct overview of game requirements.

The long-term evaluation teachers who completed all or some of the post-game debrief recalled the activity stimulated **classroom discussion between teachers and students about cyber-safety issues** and **raised awareness of cyber-safety strategies**:

> *"[The post-game debrief] summed up the detectives activity quite well. It provided a couple of avenues for the students to go off and explore if they wanted some more information."* [LT_B]
>
> *"The questioning gave a great guideline on questions to ask children."* [LT_C]

The majority of long-term evaluation teachers who did compete the post-game debrief **did not modify** any part of this activity. Those few who did modify the post-game debrief did so to best **suit their class needs**. Further, teachers mentioned there was **not anything they disliked** about the post-game activity as it presented a **good summary** of lessons learned throughout the game and provided an excellent **guide for class discussion**.

Long-term evaluation teachers who did not complete the post-game debrief indicated **time** was the most impeding factor. Notably, one short-term evaluation teacher acknowledged in hindsight they would have completed the pre- and post-game activities as *"the game was good, but we certainly could have got a lot more out of it [if we had utilised the pre and post-game resources]."* [Scl_010_ST]

4.3.5 Level of satisfaction with the CSD activity

All short- and long-term evaluation teachers unanimously agreed they would play the game again with future Year 6-7 classes as *"the game is a very good education for students and an insight for teachers"* [Scl_004_ST]. Short-term evaluation teachers also identified their **students seemed to enjoy the game**:

> *"The kids really liked the activity because they found it interactive and really liked being on a computer."* [Scl_001_ST]

Many short-term respondents commented the CSD activity provided their students with a **unique technology-based learning experience** and **encouraged students to think about cyber-safety in a practical way**:

> *"I think it was a great experience for the kids. In a way it put into practice some of the things they had been taught – it was practical and hands on. They like to be able to get onto the computer. So it's one thing to talk about it, but for them to actually do it and experience it, I think it really reinforces the safety messages that have been taught."* [Scl_005_ST]

> *"It's really important that kids are made aware of these things [cyber-safety] and how exactly do you go about that? You could scare them, but it doesn't always create the right response. It needs to be carefully thought about. I think this game does justice to that."* [Scl_006_ST]

Further, many short- and long-term respondents indicated cyber-safety is a **relevant** issue for the youth of today, with short-term evaluation teachers further commenting there **is a need** to educate students about cyber-safety due to the issue **not currently being taught in the curriculum**:

> *"Many of them do have Internet accounts, social networking, pet pal, MSN – quite a few of them even have Facebook. So they have access to those technologies, therefore need to be educated about appropriate ways to socialise online in a safer manner."* [Scl_012_ST]

A few short-term teachers also noted they would recommend the game to other teachers, however, they suggested that the game scenario is **only suitable for students in Year 5 and over**. Similarly, long-term respondents indicated the game requires **varied**

scenarios to ensure the game can be played with multiple year groups and repeated in consecutive years.

Notably, the majority of long-term evaluation teachers indicated they ***had* recommended the CSD activity** to other teachers as it was fun, *"**relevant** and worthwhile for the age group"* [LT_C]. More importantly, teachers identified the game encouraged students to **think about cyber-safety**:

> *"The kids absolutely love it [the CSD activity]… they get so involved. It's a great problem solving activity as well."* [LT_A]

Those long-term teachers who had not recommended the game to other teachers suggested the topic of cyber-safety had not arisen as a pressing need in their school or had only been discussed by ICT staff and, as a result, never required action by them.

4.3.6 Other cyber-safety initiatives

Respondents were asked to indicate how they would rate the priority their school has placed on cyber-safety this year. Almost all long-term evaluation teachers suggested their school placed a **high priority** and the majority of short-term teachers felt their school placed a **medium** or **high priority** on cyber-safety this year (2010). Short-term evaluation teachers further commented their school **highly values the need to educate both staff and students** about cyber-safety. However, these teachers noted the need is not necessarily translated into action as their **school has not instigated any cyber-safety activities with students' in their class**. Further, one teacher commented they had **rules restricting student's use of technology** at school, but did not create opportunities to educate students on why these rules are important. This suggests schools may place a high value on cyber-safety, but struggle to find appropriate opportunities to actively educate staff and students. A few short-term teachers commented their school placed a **low priority** on cyber-safety this year, noting limited or no opportunities for professional learning and development to increase teacher knowledge and understanding of the area. Given that teachers were not asked to list educational strategies by level of priority, it is unclear which issues were considered as a higher priority or more important than cyber-safety.

The majority of short-term evaluation teachers had **not undertaken any cyber-safety** activities (other than the CSD activity) with students in their class, while the majority of long-term evaluation teachers had. One long-term evaluation teacher no longer taught Year 6/7, therefore could not respond (**not applicable**). Those teachers who did complete other initiatives, indicated they integrated cyber-safety activities into **curriculum lessons** or utilised other resources produced by the ACMA, such as **CyberQuoll**. One long-term evaluation teacher also indicated their school participated in the Alannah and Madeline Foundation's **eSmart** pilot project.

4.4 Student quantitative results

This section presents the quantitative data collected with students during the pre and post-test assessments. To reduce the overall length of this section, the results are presented by age with comments regarding differences between the genders made in the appropriate section. The full break-down of results by gender is presented in Appendix 9.

Data in this section is presented for the nine schools at which pre-test and post-test surveys were completed. An information letter and consent form was sent home via the classroom teacher to 341 parents/carers in nine schools. Parents of 12 students declined to provide consent for their son/daughter to participate in the written questionnaire and 37 students were absent on the date of the CSD activity (Table 7). At pre-test, data were collected from 292 students (Table 7). A further 23 students were absent at post-test; hence, a total of 269 students completed a post-test survey.

Table 7. Student response rate

	Pre-test		Post-test	
	n	**%**	***n***	**%**
Total students	341	100	--	--
Without consent	12	3	--	--
With consent	329	96	292	100
Absent	37	11	23	8
Completed survey	292	89	269	92

NB: Those students who were absent at pre-test were not asked to complete the post-test survey

4.4.1 Demographics

Demographic questions were asked in the pre-test student questionnaire (Table 8). The age of students ranged from 10 to 13 years, with the majority of students being aged 11 (73%, *n* = 210) or 12 (25%, *n* = 71) years. Two students participated who stated they were 10 years old and were excluded from further analyses due to absence of permission to use data from these students. Moreover, due to the small number of 13-year-old students participating (*n* = 5), data for these students was excluded from further analyses. The sample comprised slightly more female (58%, *n* = 163) than male students due to one school being an all girls school. Three-quarters (77%, *n* = 216) of students live with both parents, with a smaller proportion of students living with their mother only (12%, *n* = 35) or with their mother and a stepfather/other adult male (8%, *n* = 21). Students were asked the postcode of their home address, which was then applied a SEIFA (Socio Economic Index for Australia) score which provided the average level of socio-economic status for the suburb. These data were then classified as below average or average and above, with a mean value of 100 points equalling the population mean. In this sample, 60% (*n* = 160) of students were classified as being in the 'average and above' category for socio-economic status.

Table 8. Student demographic characteristics

Characteristic		%	*n*
Age	10*	1	2
	11	73	210
	12	25	71
	13**	2	5
Gender	Male	42	117
	Female	58	163
Living status	Both parents	77	216
	Mother and stepfather/ other adult male	8	21
	Father and stepmother/ other adult female	1	2
	Mother only	12	35
	Father only	1	3
	Other guardian	1	3
Socio-economic status	Below average	40	105
	Average or above	60	160

* Ethical clearance was not attained for use of data from 10-year-old students; hence, responses provided by these students have been removed from further analyses.
** Due to the low number participating, 13-year-old students were excluded from further analyses.

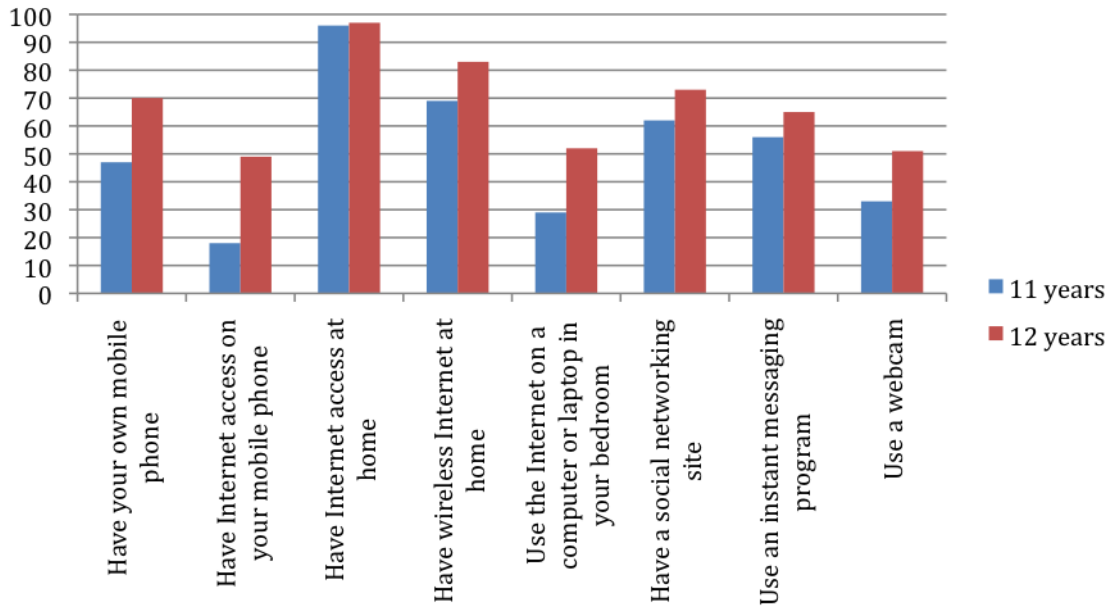
4.4.2 Technology use

Students were asked a series of questions relating to their technology use. First, students were asked about their access to technology (Table 9). Approximately half (11 years: 47%, *n* = 99; 12 years: 70%, *n* = 50) of the students surveyed reported they have their own mobile phone, with some students having Internet access on their mobile phone (11 years: 18%, *n* = 37; 12 years: 49%, *n* = 34;). Almost all students reported having access to the Internet at home (11 years: 96%, *n* = 200; 12 years: 97%, *n* = 69) and for the majority, this access was available wirelessly (11 years: 69%, *n* = 140; 12 years: 83%, *n* = 58). Interestingly, between one-third and one-half of students (11 years: 29%, *n* = 61; 12 years: 52%, *n* = 37) reported they use the Internet on a computer or laptop in their bedroom. When asked about their social contact on the Internet, approximately two-thirds of students reported having a social networking site (11 years: 62%, *n* = 131; 12 years: 73%, *n* = 52) whereas approximately half of students reported they use an instant messaging program (11 years: 56%, *n* = 118; 12 years: 65%, *n* = 46) and between one-third and one-half of students reported using a webcam (11 years: 33%, *n* = 70; 12 years: 51%, *n* = 36). More girls than boys had their own mobile (56% versus 48%), wireless Internet access at home (75% versus 69%), use a SNS or IM program (69% versus 60% and 61% versus 55%).

Table 9. Students' technology use

	11 years		12 years	
	Yes % (*n*)	**No** % (*n*)	**Yes** % (*n*)	**No** % (*n*)
Have your own mobile phone	47 (99)	53 (111)	70 (50)	30 (21)
Have Internet access on your mobile phone	18 (37)	82 (171)	49 (34)	51 (36)
Have Internet access at home	96 (200)	4 (8)	97 (69)	3 (2)
Have wireless Internet at home	69 (140)	31 (63)	83 (58)	17 (12)
Use the Internet on a computer or laptop in your bedroom	29 (61)	71 (149)	52 (37)	48 (34)
Have a social networking site	62 (131)	38 (79)	73 (52)	27 (19)
Use an instant messaging program	56 (118)	44 (92)	65 (46)	35 (25)
Use a webcam	33 (70)	67 (140)	51 (36)	49 (35)

Figure 2. Students' technology use



Students were then asked about the frequency with which they made and received phone calls (Table 10) and sent text messages on an average school day, before and after school and on the weekend (Table 11). Approximately half of 11-year-old students reported they do not have a mobile phone (54%, *n* = 112), whereas one-third of 12-year-old students do not have a mobile phone (31%, *n* = 21). Of those who do, the majority of students reported they did not receive or make phone calls on an **average day at school** (11 years: 35%, *n* = 72; 12 years: 53%, *n* = 36), followed by one to three calls per day (11 years: 11%, *n* = 22; 12 years: 12%, *n* = 8). Approximately one-quarter of students reported they made or received no phone calls on an **average day before or after school** (11 years: 25%, *n* = 52; 12 years: 27%, *n* = 19), with a similar number of students reporting they made or received between one and three phone calls (11 years: 18%, *n* = 38; 12 years: 32%, *n* = 23) during this time period. One-fifth of students reported making or receiving no phone calls per day on an **average day of the weekend** (11 years: 19%, *n* = 39; 12 years: 19%, *n* = 13) with slightly fewer 11-year-old and slightly more 12-year-old students reporting they made or received between one and three phone calls (11 years: 17%, *n* = 35; 12 years: 27%, *n* = 19) in this period of time. Overall, girls reported making or receiving more phone calls on an average day at school and before or after school than boys (14% versus 6% and 26% versus 16% respectively).

When asked about the frequency with which they sent text messages, again, the majority of 11-year-old students reported they did not have a mobile phone (55%, *n* = 114)

while 32% (*n* = 22) of 12-year-old students reported this (Table 11). Of those who do, the majority reported sending less than five text messages on their mobile phone on an **average day at school** (11 years: 39%, *n* = 81; 12 years: 64%, *n* = 44). On an **average day before or after school**, over one-third of students reported sending less than five text messages on their mobile phone (11 years: 35%, *n* = 74; 12 years: 47%, *n* = 33), followed by between six and 10 text messages (11 years 5%, *n* = 10; 12 years: 11%, *n* = 8) and 11 to 15 text messages (11 years: 3%, *n* = 6; 12 years: 6%, *n* = 4). Responses to the question about text message use on an **average day on the weekend** were more varied. Just over one-quarter of students reported they send less than five text messages on an average day on the weekend (11 years: 25%, *n* = 52; 12 years: 34%, *n* = 24), while 11% (*n* = 22) of 11-year-old and 12-year-old students (*n* = 8) reported sending between six and 10 text messages, 4% (*n* = 8) of 11-year-old and 9% (*n* = 6) of 12-year-old students reported sending 11 to 15 text messages and 3% (*n* = 6) of 11-year-olds and 11% (*n* = 8) of 12-year-olds reported sending more than 20 text messages on an average day of the weekend.

Table 10. Frequency of calls made and received on students' mobile phone

	11 years % (*n*)						12 years % (*n*)					
	Don't have mobile	**None**	**1-3**	**4-5**	**6-10**	**10+**	**Don't have mobile**	**None**	**1-3**	**4-5**	**6-10**	**10+**
Average school day	54 (112)	35 (72)	11 (22)	1 (1)	0 (0)	0 (0)	31 (21)	53 (36)	12 (8)	3 (2)	2 (1)	0 (0)
Average day before or after school	53 (109)	25 (52)	18 (38)	3 (6)	1 (2)	0 (0)	30 (21)	27 (19)	32 (23)	7 (5)	1 (1)	3 (2)
Average weekend day	53 (109)	19 (39)	17 (35)	8 (16)	2 (5)	1 (3)	29 (20)	19 (13)	27 (19)	13 (9)	4 (3)	9 (6)

Table 11. Frequency of text messages sent on students' mobile phone

	11 years % (*n*)						12 years % (*n*)					
	Don't have mobile	**Less than 5**	**6-10**	**11-15**	**16-20**	**20+**	**Don't have mobile**	**Less than 5**	**6-10**	**11-15**	**16-20**	**20+**
Average school day	55 (114)	39 (81)	4 (8)	1 (1)	0 (0)	1 (2)	32 (22)	64 (44)	3 (2)	1 (1)	0 (0)	0 (0)
Average day before or after school	54 (112)	35 (74)	5 (10)	3 (6)	1 (1)	2 (3)	30 (21)	47 (33)	11 (8)	6 (4)	1 (1)	4 (3)
Average weekend day	54 (112)	25 (52)	11 (22)	4 (8)	3 (6)	3 (6)	31 (22)	34 (24)	11 (8)	9 (6)	3 (2)	11 (8)

Figure 3. Frequency of calls made and received on students' mobile phone

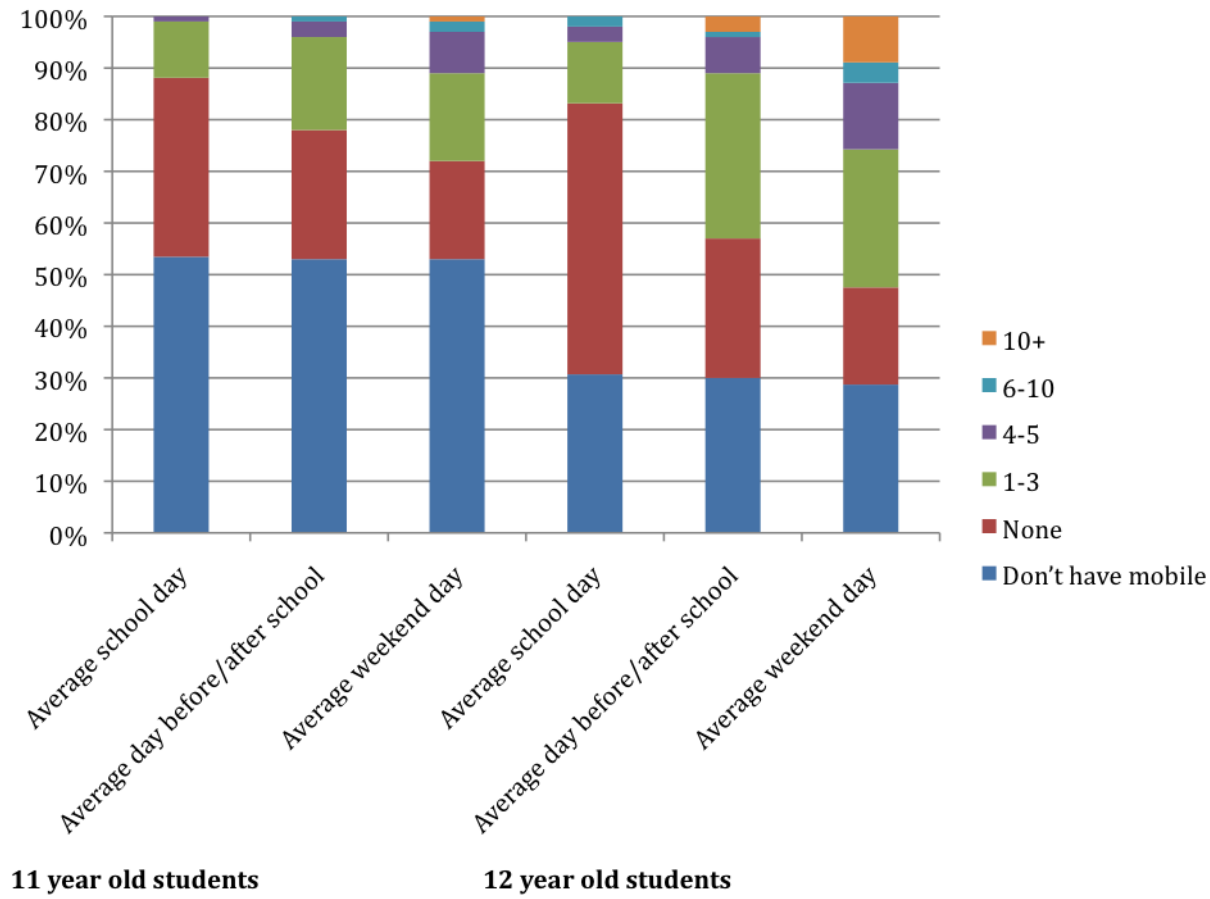
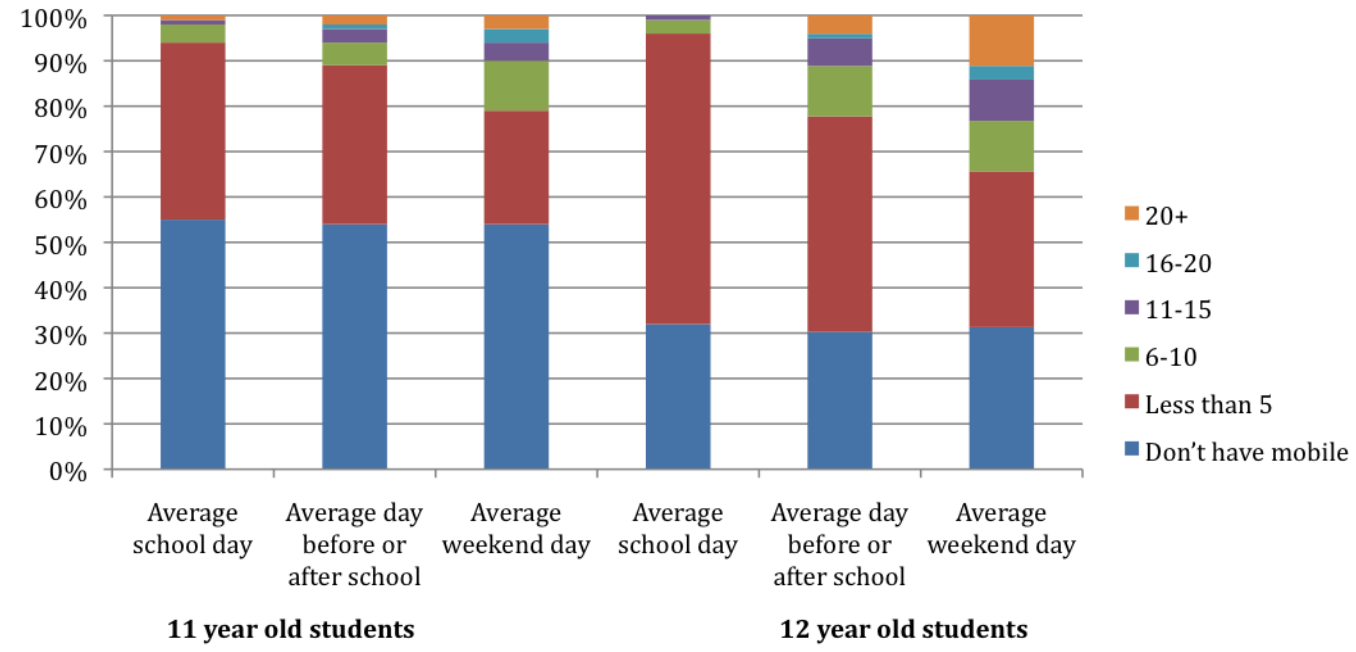


Figure 4. Frequency of text messages sent on students' mobile phone



Students were next asked how many times a day they used the Internet on their mobile phone (Table 12). Of the 47% of 11-year-old and 71% of 12-year-old students who have a mobile phone, the majority of students reported they did not use the Internet on their mobile phone on an **average day at school**, with 8% (*n* = 16) of 11-year-old and 10% (*n* = 7) of 12-year-old students reporting they used the Internet on their mobile phone one to three times. Again, the majority of students reported they did not have a mobile phone or that they did not use the Internet on their mobile phone on an **average day before and after school** and 9% (*n* = 19) of 11-year-old and 15% (*n* = 10) of 12-year-old students reported using the Internet on their mobile phone between one and three times in this time period. Finally, 7% (*n* = 15) of 11-year-old and 21% (*n* = 15) of 12-year-old students reported using the Internet on their mobile phone between one and three times on an **average day of the weekend**.

Finally, students were asked to describe their Internet use on an average weekday and an average day of the weekend, for school work and not for school work (Table 13). Over one-third of students reported using the Internet for less than one hour on an **average week day for school work** (11 years: 43%, *n* = 90; 12 years: 39%, *n* = 27), with about one-third of students (11 years: 35%, *n* = 72; 12 years: 29%, *n* = 20) reporting they use the Internet for about an hour for school work on an average day of the week. When asked about the time spent using the Internet **on an average day of the week not for school work**, approximately one-third reported spending less than one hour (11 years: 33%, *n* = 69; 12 years: 23%, *n* = 16) and a further one-third reported spending about an hour (11 years: 30%, *n* = 63; 12 years: 30%, *n* = 21).

Just under half of students reported using the Internet for less than one hour on an **average day of the weekend for school work** (11 years: 42%, *n* = 86; 12 years: 43%, *n* = 30), followed by about one hour (11 years: 31%, *n* = 64; 12 years: 21%, *n* = 15), two hours (11 years: 11%, *n* = 23; 12 years: 13%, *n* = 9) and three hours (11 years: 5%, *n* = 11; 12 years: 6%, *n* = 4). Students' report of Internet use on an **average day of the weekend not for school work** was more varied than responses to other time use questions. Approximately one-fifth of students reported each of the following: less than one hour (11 years: 21%, *n* = 44; 12 years: 18%, *n* = 12), about one hour (11 years: 22%, *n* = 47; 12 years: 22%, *n* = 15) and about two hours (11 years: 21%, *n* = 44; 12 years: 21%, *n* = 14), while 12% (*n* = 25) of 11-year-old and 15% (*n* = 10) of 12-year-old students reported using the Internet for about three hours, 4% (*n* = 9) of 11-year-old and 7% (*n* = 5) of 12-year-old students for about four hours and 8% (*n* = 17) of 11-year-old and 15% (*n* = 10) of 12-year-old students for more than four hours on an average day of the weekend not for school work.

Table 12. Frequency of Internet use on students' mobile phone

	11 years % (*n*)						12 years % (*n*)					
	Don't have mobile	**None**	**1-3 times**	**4-5 times**	**6-10 times**	**10+ times**	**Don't have mobile**	**None**	**1-3 times**	**4-5 times**	**6-10 times**	**10+ times**
Average school day	53 (110)	38 (79)	8 (16)	0 (0)	0 (0)	2 (1)	29 (20)	57 (39)	10 (7)	0 (0)	2 (1)	2 (1)
Average day before or after school	52 (108)	35 (72)	9 (19)	2 (4)	1 (2)	1 (2)	29 (20)	46 (32)	15 (10)	6 (4)	1 (1)	3 (2)
Average weekend day	52 (108)	30 (61)	7 (15)	6 (12)	3 (6)	2 (4)	30 (21)	33 (23)	21 (15)	7 (5)	1 (1)	7 (5)

Table 13. Frequency of students' Internet use

	11 years % (*n*)							12 years % (*n*)						
% (n)	**Don't use Internet**	**Less than 1 hour**	**About 1 hour**	**About 2 hours**	**About 3 hours**	**About 4 hours**	**More than 4 hours**	**Don't use Internet**	**Less than 1 hour**	**About 1 hour**	**About 2 hours**	**About 3 hours**	**About 4 hours**	**More than 4 hours**
For school work:														
Average week day	4 (8)	43 (90)	35 (72)	14 (29)	2 (5)	1 (3)	0 (0)	6 (4)	39 (27)	29 (20)	19 (13)	3 (2)	0 (0)	4 (3)
Average weekend day	9 (19)	42 (86)	31 (64)	11 (23)	5 (11)	1 (2)	1 (1)	13 (9)	43 (30)	21 (15)	13 (9)	6 (4)	1 (1)	3 (2)
NOT for school work:														
Average week day	11 (22)	33 (69)	30 (63)	17 (36)	5 (11)	1 (3)	2 (4)	6 (4)	23 (16)	30 (21)	16 (11)	10 (7)	6 (4)	9 (6)
Average weekend day	11 (23)	21 (44)	22 (47)	21 (44)	12 (25)	4 (9)	8 (17)	3 (2)	18 (12)	22 (15)	21 (14)	15 (10)	7 (5)	15 (10)

Figure 5. Frequency of 11-year-old students' Internet use

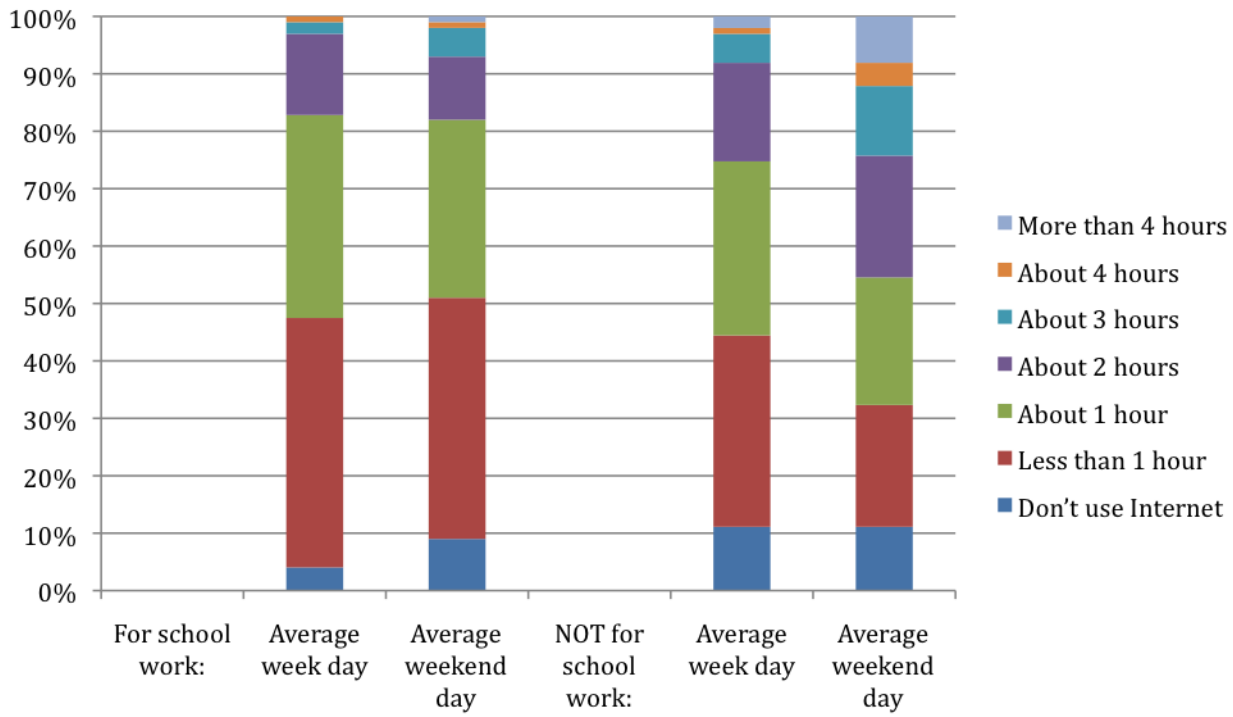
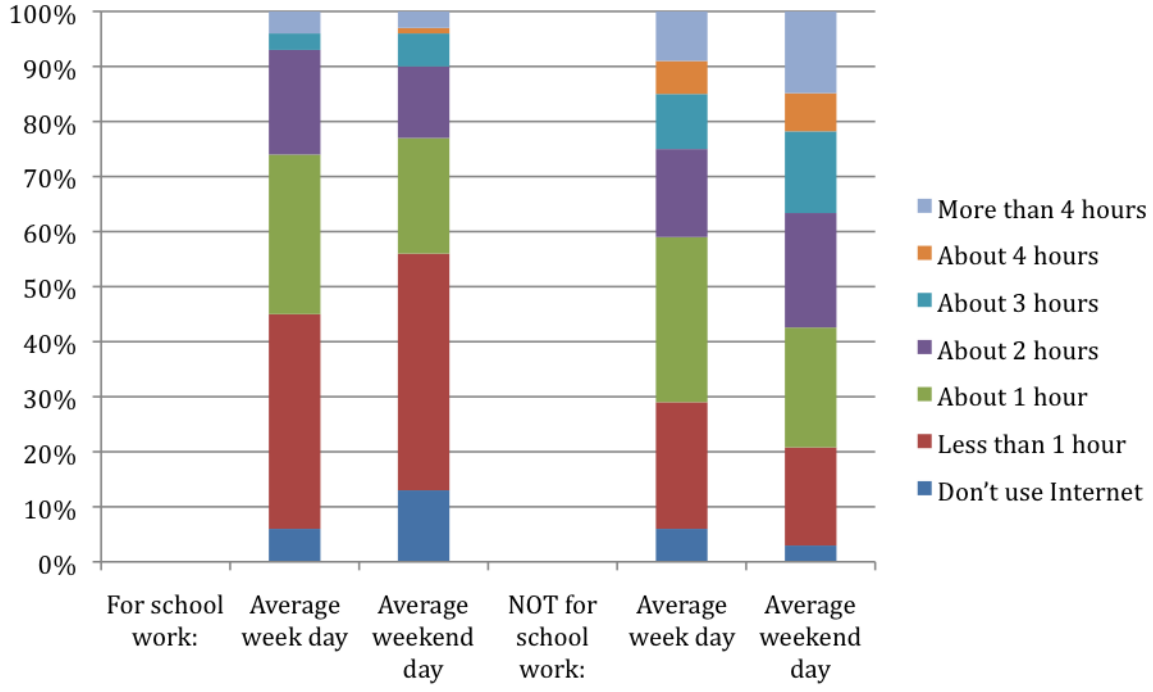


Figure 6. Frequency of 12-year-olds Internet use



4.4.3 Location of Internet use

Students were asked to report where they usually use the Internet and provided with a list of responses from which to choose (Table 14). Students could choose more than one response to this question. The majority of students reported they usually used the Internet at home (11 years: 93%, *n* = 194; 12 years: 94%, *n* = 67) or at school (11 years: 51%, *n* = 107; 12 years: 49%, *n* = 35), while fewer students reported using the Internet at a friends' house (11 years: 26%, *n* = 54; 12 years: 27%, *n* = 19), at the library (11 years: 12%, *n* = 25; 12 years: 27%, *n* = 19) or at other places (e.g. another family member's house, their parents work or on a mobile phone) (11 years: 7%, *n* = 15; 12 years: 10%, *n* = 7).

Table 14. Location of Internet use

	11 years % (*n*)	**12 years** % (*n*)
I do not use the Internet	1 (3)	0 (0)
At home	93 (194)	94 (67)
At school	51 (107)	49 (35)
At a friends' house	26 (54)	27 (19)
At the library	12 (25)	27 (19)
Other	7 (15)	10 (7)

NB: Students could select more than one response

Students were then asked where at home they usually use the Internet (Table 15). Again, students could choose more than one response to this question. Half of students reported using the Internet at home in an open area (11 years: 50%, *n* = 105; 12 years: 58%, *n* = 41), with a similar number of students reporting they usually used the Internet in the study or a separate room at home (11 years: 55%, *n* = 115; 12 years: 56%, *n* = 40). Between one-quarter and one-half of students reported they usually used the Internet in their bedroom (11 years: 22%, *n* = 46; 12 years: 42%, *n* = 30).

Table 15. Location of Internet use <u>at home</u>

	11 years % (*n*)	**12 years** % (*n*)
I do not use the Internet at home	4 (9)	1 (1)
In an open area (e.g. lounge room, kitchen)	50 (105)	58 (41)
In my bedroom	22 (46)	42 (30)
In the study or separate room	55 (115)	56 (40)
In the bathroom	0 (0)	3 (2)
Other	5 (10)	4 (3)

NB: Students could select more than one response

Students were asked to list their three favourite websites. The five most common chat sites used by students in this sample are presented in Table 16. A full list of websites and the frequency with which they were visited, is presented in Appendix 7.

Table 16. Common Internet sites

	11 years		**12 years**	
	%	n	%	n
Facebook	27	57	42	30
MSN	25	53	28	20
YouTube	14	30	15	11
Club Penguin	13	27	13	9
Hotmail / Yahoo / Gmail	13	27	3	2

4.4.4 Social networking site use

Over two-thirds of 11 (70%) and 12 (74%) year old students reported they use a social networking site (e.g., Facebook, MySpace, Club Penguin) or Instant Messenger (e.g., MSN) (Table 17). For 11-year-old students, the most commonly used site was MSN (44%, n=93), followed by Facebook (34%, *n* = 72) and Club Penguin (28%, *n* = 59) (Table 12). MSN was also the most popular site for 12-year-old students (52%, *n* = 37), followed closely by Facebook (49%, *n* = 35), then Club Penguin (31%, *n* = 22).

Table 17. Type of social networking site or Instant Messenger used

	11 years % (*n*)	**12 years** % (*n*)
I do not use this	26 (55)	21 (15)
Club Penguin	28 (59)	31 (22)
Bebo	2 (4)	4 (3)
MySpace	5 (11)	13 (9)
Facebook	34 (72)	49 (35)
MSN	44 (93)	52 (37)
Twitter	2 (5)	7 (5)
Other	19 (40)	14 (10)

NB: Students could select more than one response

Students were asked about the frequency with which they use a social networking site (SNS) or instant messenger (IM) site on an average day at school, before or after school and on the weekend (Table 18). Perhaps due to restricted access to these sites during school hours, more students reported they 'did not have this' to the question about frequency of use of SNS or IM on an average day at school (11 years: 64%, *n* = 127; 12 years: 62%, *n* = 43), compared to the previous question about individual site usage (11 years: 26%, *n* = 55; 12 years: 21%, *n* = 15). Of those who do use these sites at school, most students reported they used the site for less than half an hour on an **average day at school** (11 years: 29%, *n* = 57; 12 years: 26%, *n* = 18). Most students who use a SNS or IM also reported using this for less than half an hour on an **average day before or after school** (11 years: 34%, *n* = 70; 12 years: 27%, *n* = 19). Use of SNS and IM is more varied on an **average weekend day**. While about one-fifth (11 years: 20%, *n* = 42; 12 years: 13%, *n* = 9) of students

reported they used these sites for less than half an hour on an average day of the weekend, a further one-fifth (11 years: 20%, *n* = 41; 12 years: 17%, *n* = 12) reported using these sites for about one hour, and a similar proportion of students used the sites for about half an hour (11 years: 12%, *n* = 24; 12 years: 17%, *n* = 12) and about two hours (11 years: 9%, *n* = 19; 12 years: 16%, *n* = 11).

Students were asked a series of questions about actions they had taken in relation to their SNS and Internet use (Table 19). At pre-test, the majority of students reported they do not have online friends whom they have not met in person (11 years: 59%, *n* = 121; 12 years: 67%, *n* = 46), they have set their SNS profile to private (11 years: 52%, *n* = 105; 12 years: 48%, *n* = 32), they have not shared their password with others (11 years: 63%, *n* = 129; 12 years: 75%, *n* = 52). Interestingly, nearly half of 11-year-olds and the majority of 12-year-olds reported that they have blocked or deleted someone who said something they think is rude or mean (11 years: 49%, *n* = 100; 12 years: 56%, *n* = 32). Furthermore, they have not shared personal details with others (11 years: 41%, *n* = 84; 12 years: 44%, *n* = 30) and they have let their parents know who is on their friends list (11 years: 49%, *n* = 100; 12 years: 56%, *n* = 39).

4.4.5 Pre and post-test administration: Differences in duration between test administrations

The duration between pre and post-test was not standardised which resulted in differences between the interval between test administrations. Three schools (*n* = 65 students) completed the post-test 14 days following the CSD activity while 11 schools (*n* = 200 students) completed the post-test 7 or 8 days after first playing the game. Importantly, at pre-test, there was no significant differences between students in the 14 days to post-test group and the 7-8 days to post-test group on these variables. Cross tabulations were calculated for each post-test question asked in the survey by the time lag between game and post-test (2 groups: those who did survey 14 days post-game and those who did survey 7/8 days post-game administration).

The only statistically significant differences (Pearson's chi-square test) were found in the following:

1. The number of students who reported they would talk to a friend if they were contacted online/on phone by someone they did not know offline (*p* = 0.050). Three-quarters (78%) of

students in the 14 days to post-test group said they would speak to a friend, compared to 65% of students in the 7-8 days to post-test group.

2. The number of students who said they would not open the messages they were sent by an unknown person (p = 0.007). Again, more 14 days to post-test students (88%) reported they would do this compared to 7-8 days to post-test students (71%).

3. The number of students who said they had been contacted on their webcam by someone unknown to them (p = 0.047). However, 7 cells had an expected count less than 5 so this result is likely to relate to sample size and should not be interpreted.

At post-test, the proportion of students who reported each of these actions was similar to pre-test results. In particular, fewer 11-year-old students reported having shared their password with others (13% at pre-test versus 6% at post-test), and more reported they have not shared their personal details with anyone (41% at pre-test versus 46% at post-test) and have let their parent/carer know who is on their friends list (49% at pre-test versus 54% at post-test). Fewer 12-year-old students have let their parent/carer know who is on their friends list (56% at pre-test versus 48% at post-test), however more 12-year-old students reported at post-test they had set their profile to private (48% at pre-test versus 53% at post-test) and they had not shared personal details with anyone (44% at pre-test versus 51% at post-test).

Table 18. Frequency of students' social networking or instant messenger site use

	11 years % (n)							12 years % (n)						
	Don't have this	Less than half an hour	About half hour	About 1 hours	About 2 hours	About 3 hours	4 hours or more	Don't have this	Less than half an hour	About half hour	About 1 hours	About 2 hours	About 3 hours	4 hours or more
Average school day	64 (127)	29 (57)	4 (8)	2 (5)	1 (1)	0 (0)	0 (0)	62 (43)	26 (18)	9 (6)	1 (1)	0 (0)	1 (1)	0 (0)
Average day before or after school	37 (74)	34 (70)	15 (30)	6 (13)	6 (12)	1 (2)	1 (2)	27 (19)	27 (19)	16 (11)	19 (13)	7 (5)	1 (1)	1 (1)
Average weekend day	29 (60)	20 (42)	12 (24)	20 (41)	9 (19)	6 (13)	3 (7)	24 (17)	13 (9)	17 (12)	17 (12)	16 (11)	10 (7)	4 (3)

Table 19. Actions taken on social networking or instant messenger site

	Pre-test						Post-test					
	11 years % (n)			12 years % (n)			11 years % (n)			12 years % (n)		
	Yes	No	Don't use	Yes	No	Don't use	Yes	No	Don't use	Yes	No	Don't use
I only have online friends that I have met in person	59 (121)	15 (32)	26 (54)	67 (46)	19 (13)	14 (10)	59 (114)	15 (29)	26 (51)	63 (41)	18 (12)	18 (12)
I have set my profile to private	52 (105)	20 (40)	28 (56)	48 (32)	33 (22)	19 (13)	52 (101)	17 (34)	30 (59)	53 (34)	25 (16)	22 (14)
I have shared my password with others	13 (26)	63 (129)	24 (49)	9 (6)	75 (52)	16 (11)	6 (77)	69 (134)	25 (49)	11 (7)	74 (48)	15 (10)
I have blocked or deleted someone who said something I think is rude or mean	49 (100)	23 (47)	28 (56)	56 (32)	37 (26)	17 (12)	53 (102)	18 (35)	29 (55)	52 (34)	29 (19)	18 (12)
I have not shared my personal details with anyone	41 (84)	36 (73)	23 (48)	44 (30)	40 (27)	16 (11)	46 (88)	29 (57)	25 (48)	51 (33)	31 (20)	18 (12)
I let my parents/caregivers know who is on my friends list	49 (100)	25 (51)	25 (51)	56 (39)	26 (18)	17 (12)	54 (104)	20 (38)	26 (51)	48 (31)	34 (22)	18 (12)

Figure 7. Actions taken by 11-year-olds on a social networking or instant messenger site

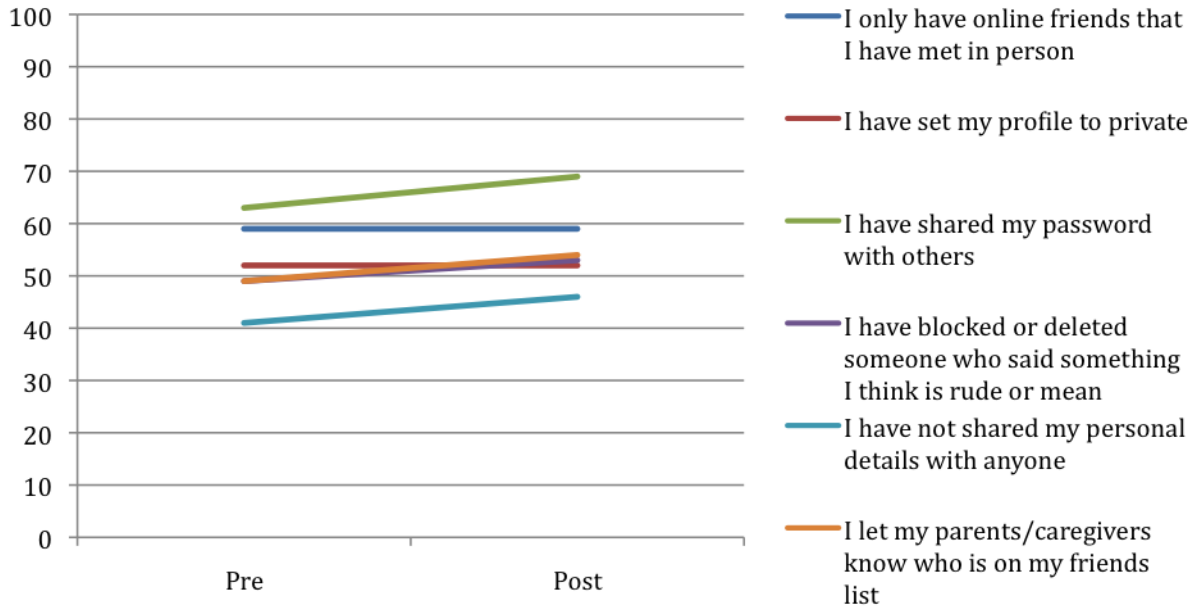
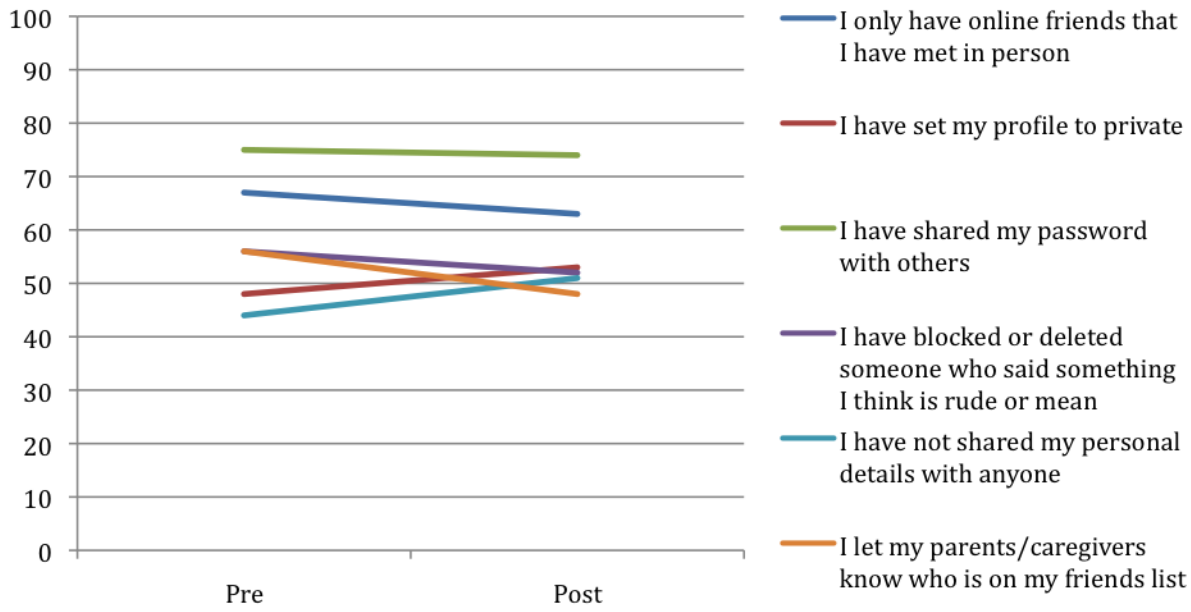


Figure 8. Actions taken by 12-year-olds on a social networking or instant messenger site



When asked the highest number of friends or contacts they have on their SNS or IM (Table 20), approximately one-quarter of students reported they did not use these sites (11 years: 28%, *n* = 59; 12 years: 20%, *n* = 14) and about one-quarter reported they had between zero and 19 friends/contacts (11 years: 22%, *n* = 46; 12 years: 24%, *n* = 17). Just under one-fifth of students had 20-49 friends (11 years: 19%, *n* = 40; 12 years: 14%, *n* = 10) and 50-99 friends (11 years: 17%, *n* = 35; 12 years: 18%, *n* = 13), with smaller numbers of students reporting higher friend/contact counts. Students were then asked what proportion of their friends/contacts list were known to them offline (Table 21). Most students reported they know all of their friends/contacts offline (11 years: 38%, *n* = 79; 12 years: 41%, *n* = 29), of those who report having a SNS or IM (*n* = 212), this equates to 51%.

Table 20. Number of friends on social networking and instant messaging sites

	11 years		12 years	
	%	*n*	%	*n*
I do not have any of these accounts	28	59	20	14
0-19	22	46	24	17
20-49	19	40	14	10
50-99	17	35	18	13
100-149	7	15	10	7
150-199	2	4	7	5
200-299	3	7	6	4
300 or more	1	3	1	1

Table 21. Proportion of online friends known offline

	11 years		12 years	
	%	*n*	%	*n*
I don't have/use this	25	53	21	15
None	4	8	3	2
About half	13	27	10	7
Nearly all	20	42	25	18
All	38	79	41	29

Figure 9. Number of friends on social networking and instant messaging sites

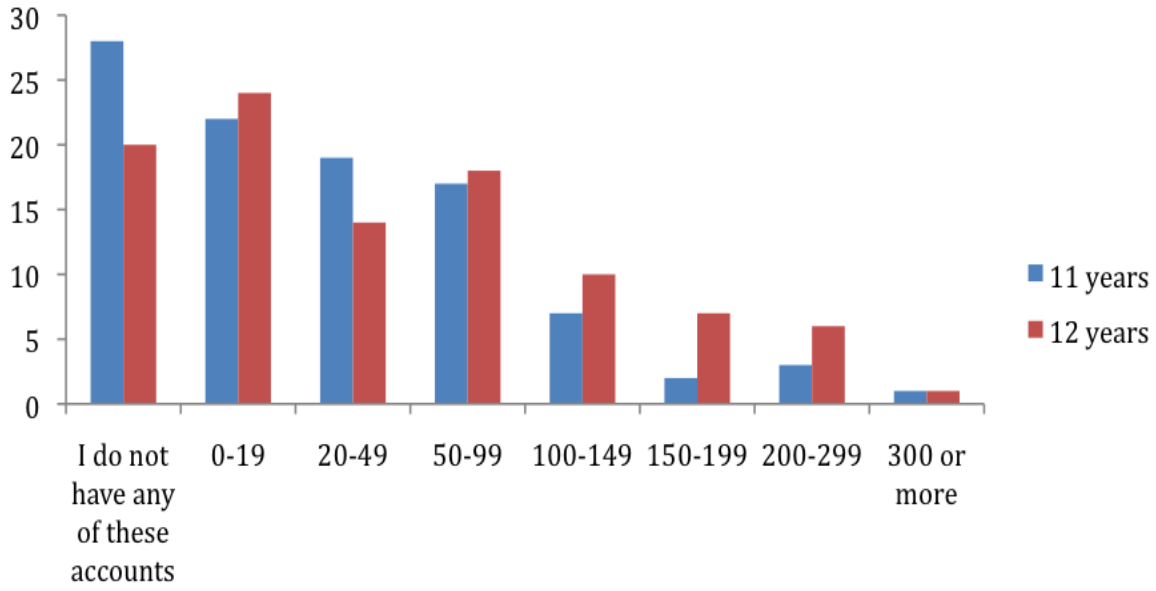
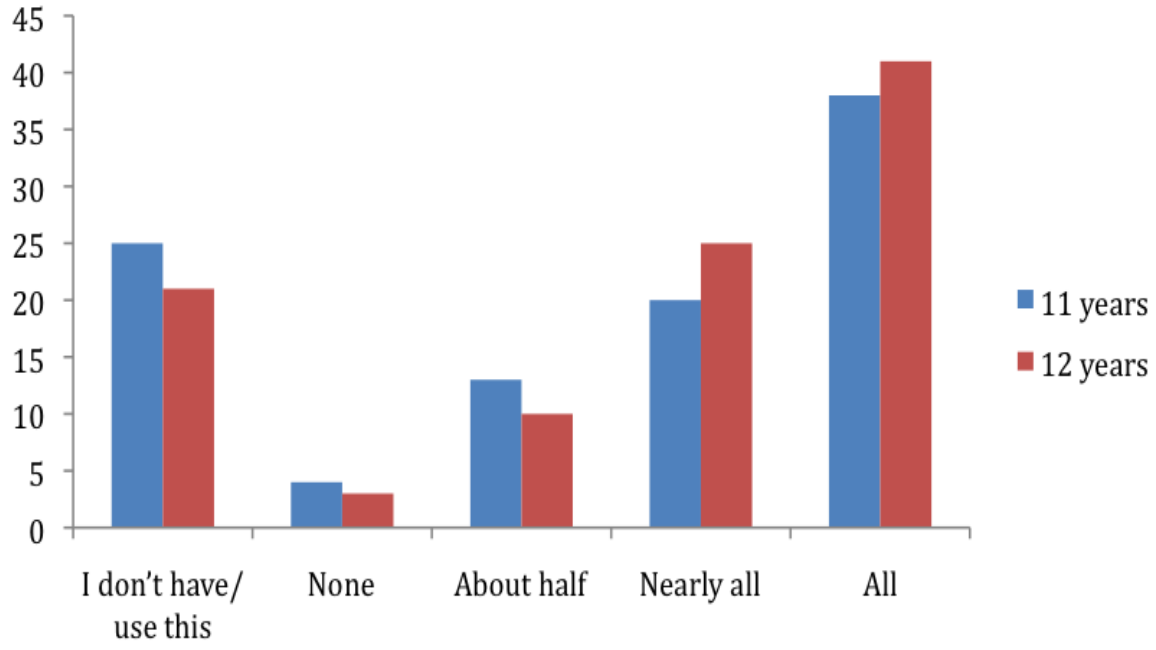


Figure 10. Proportion of online friends known offline



4.4.6 Chat site use

Students were asked to list up to three chat sites they used on the Internet. Between one-quarter and one-third of students (11 years: 37%; 12 years: 26%) reported they do not use chat sites on the Internet. Of those who do (11 years: 57%, *n* = 118; 12 years: 73%, *n* = 50), the five most common chat sites used are described in Table 22.

Table 22. Common Internet chat sites

	11 years		12 years	
	%	*n*	%	*n*
MSN / Meebo / EBuddy	35	74	44	31
Facebook	30	62	45	32
Club Penguin	12	25	11	8
Hotmail / Yahoo / Gmail	11	23	6	4
MySpace	4	8	7	5

4.4.7 Online game use

The majority of students reported they play games on the Internet (e.g., World of Warcraft) (11 years: 76%, *n* = 155; 12 years: 88%, *n* = 58). Amongst these students, the most popular mode of online game playing was via a computer (11 years: 71%, *n* = 149; 12 years: 75%, *n* = 53), with much smaller numbers of students reporting using other consoles for example, Nintendo DSi (11 years: 26%, *n* = 55; 12 years: 28%, *n* = 20), PlayStation including PS2 and PS3 (11 years: 20%, *n* = 43; 12 years: 20%, *n* = 14) and Xbox (11 years: 10%, *n* = 21; 12 years: 22%, *n* = 16) (Table 23).

Table 23. Online game use

	11 years		12 years	
	%	n	%	n
I do not play online games	17	35	10	7
Nintendo DSi / DS / DS Lite	26	55	28	20
PlayStation Portable (PSP)	7	14	15	11
PlayStation (e.g. PS2, PS3)	20	43	20	14
Xbox	10	21	22	16
Computer	71	149	75	53
Other:	19	40	18	13
Wii	10	21	7	5
Mobile phone	1	1	3	2
iPod / iTouch	3	6	3	2

NB: Students could select more than one response

When playing online games, one-quarter of students play games without interacting with others online (11 years: 28%, *n* = 57; 12 years: 28%, *n* = 18) (Table 24). A further one-quarter of students report playing online games with only people they have met in person (11 years: 23%, *n* = 46; 12 years: 20%, *n* = 13) and almost one-third reported playing online games with both others whom they have and have not met in person (11 years: 32%, *n* = 64; 12 years: 40%, *n* = 26).

Table 24. Online game contacts

	11 years		12 years	
	%	*n*	%	*n*
ONLY people you have met in person	23	46	20	13
ONLY people you have never met	1	1	0	0
BOTH people you know in person and people you have never met	32	64	40	26
I don't play games online with any other person	28	57	28	18
I don't play online games	17	34	12	8

4.4.8 Contact with unknown other

Students were asked to report the frequency with which they have ever been contacted online by someone whom they have not met in person (Tables 25 and 26). The majority of students reported they either did not have a **SNS** (11 years: 35%, *n* = 70; 12 years: 24%, *n* = 17) or that they had not been contacted by someone they have not met in person on this site (11 years: 32%, *n* = 64; 12 years: 40%, *n* = 28). Smaller numbers of students reported some contact on their social networking site by someone they have not met, ranging from once (11 years: 8%, *n* = 17; 12 years: 14%, *n* = 10) to more than five times (11 years: 8%, *n* = 16; 12 years: 9%, *n* = 6). At post-test, the proportion of 12-year-old students who reported having been contacted on their social networking site by someone they have not met in person increased (at pre-test 33% had any contact versus 37% at post-test) (Table 20).

Nearly half of 11-year-old (44%, *n* = 88) and one-third of 12-year-old (33%, *n* = 23) students in this study did not use **MSN**; however, among those who do, most students (11 years: 35%, *n* = 70; 12 years: 44%, *n* = 31) report never having received contact by someone they have not met in person. The frequency of students' report of contact on MSN by someone they have not met in person displayed a negative trend (i.e., increasingly fewer students reported higher levels of contact with someone whom they had not met in person). At post-test, the frequency with which 11-year-old students reported being contacted on MSN by someone they don't know two to three times rose to 10% (from 4% at pre-test). Moreover, the frequency with which 12-year-old students reported being contacted on MSN only once increased from 9% to 15% and contact more than five times rose from 4% at pre-test to 10% at post-test.

Almost all students reported they either did not use a **webcam** (11 years: 55%, *n* = 110; 12 years: 44%, *n* = 31) or that they had never been contacted by someone they had not met in person on their webcam (11 years: 42%, *n* = 84; 12 years: 49%, *n* = 34).

Over 70% of students reported they either did not have a **mobile phone** (11 years: 55%, *n* = 110; 12 years: 33%, *n* = 23) or that they had never been contacted by someone they had not met in person on their mobile phone (11 years: 31%, *n* = 63; 12 years: 37%, *n* = 26). Smaller numbers of students reported some contact: 8% (*n* = 15) of 11-year-old and 11% (*n* = 8) of 12-year-old students reported being contacted once, 3% (*n* = 7) of 11-year-old and 14% (*n* = 10) of 12-year-old students reported being contacted two to three times,

2% (*n* = 4) of 11-year-old students reported being contacted four to five times and 1% (*n* = 1) of 11-year-old and 4% (*n* = 3) of 12-year-old students reported being contacted more than five times on their mobile phone by someone they have not met in person. The proportion of 11-year-old students who reported being contacted only once on their mobile phone by someone they had not met rose from pre-test to post-test (8% to 11% respectively). The proportion of 12-year-old students who reported being contacted only once (11% to 9%) and two to three times (14% to 6%) dropped between pre- and post-tests, while the proportion of students reporting contact four to five times increased from 0% at pre-test to 8% at post-test.

At pre-test, most students had not used (11 years: 47%, *n* = 92; 12 years: 32%, *n* = 22) nor been contacted (11 years: 36%, *n* = 72; 12 years: 48%, *n* = 33) on a **chat site** by someone they had not met in person. At pre-test, 16% (*n* = 34) of 11-year-old and 29% (*n* = 21) of 12-year-old students had been contacted by someone they did not know in person on a chat site once. For 11-year-olds, this increased at post-test to 19% (*n* = 39) and for 12-year-olds, more frequent contact was reported with the proportion of students citing contact more than five times rising from 6% (*n* = 4) at pre-test to 16% (*n* = 10) at post-test.

The majority of students reported they either did not have/use a **blog** (11 years: 53%, *n* = 127; 12 years: 49%, *n* = 34) or that they had never been contacted on their blog by someone they had not met in person (11 years: 29%, *n* = 59; 12 years: 46%, *n* = 32).

While two-thirds of students reported they had never been contacted in an **online game** by someone they had not met in person (11 years: 38%, *n* = 76; 12 years: 51%, *n* = 36) or they did not use/have online games (11 years: 34%, *n* = 68; 12 years: 10%, *n* = 7), some students had experienced contact. For 11-year-old students, report of contact two to three times rose from 4% (*n* = 8) at pre-test to 8% (*n* = 16) at post-test and for 12-year-old students report of contact four to five times rose from 1% (*n* = 1) at pre-test to 5% (*n* = 3) at post-test.

Students who said they had been contacted in other ways by someone they did not know in person most frequently cited this was through **email** (11 years: 1%, *n* = 3; 12 years: 1%, *n* = 1).

Table 25. Frequency of contact by someone 11-year-old student has not met in person

	Pre-test % (*n*)						Post-test % (*n*)					
	Don't have/use	**Never**	**Only 1 time**	**2-3 times**	**4-5 times**	**More than 5 times**	**Don't have/use**	**Never**	**Only 1 time**	**2-3 times**	**4-5 times**	**More than 5 times**
Social networking site	35 (70)	32 (64)	8 (17)	13 (27)	4 (7)	8 (16)	34 (67)	28 (55)	8 (18)	17 (34)	4 (7)	8 (15)
Instant messenger	44 (88)	35 (70)	9 (18)	4 (9)	5 (11)	3 (6)	42 (81)	32 (62)	9 (17)	11 (21)	2 (3)	4 (7)
Webcam	55 (110)	42 (84)	1 (1)	1 (1)	1 (2)	2 (3)	58 (112)	35 (68)	3 (6)	2 (4)	1 (3)	1 (1)
Mobile phone	55 (110)	31 (63)	8 (15)	3 (7)	2 (4)	1 (1)	54 (105)	29 (57)	9 (18)	4 (8)	1 (1)	2 (4)
Chat room	47 (92)	36 (72)	4 (8)	5 (10)	2 (3)	7 (13)	51 (99)	29 (56)	8 (15)	6 (12)	2 (4)	4 (8)
Blog	53 (127)	29 (59)	6 (11)	1 (2)	0 (0)	1 (2)	61 (116)	32 (62)	1 (2)	4 (8)	1 (1)	1 (2)
Online game	34 (68)	38 (76)	7 (15)	4 (8)	5 (10)	12 (23)	32 (61)	36 (68)	9 (18)	8 (16)	2 (4)	12 (24)
Other	--	5 (10)	1 (1)	1 (2)	1 (1)	1 (1)	91 (190)	5 (11)	2 (4)	1 (2)	0 (0)	1 (2)

Table 26. Frequency of contact by someone 12-year-old student has not met in person

	Pre-test % (*n*)						Post-test % (*n*)					
	Don't have/use	**Never**	**Only 1 time**	**2-3 times**	**4-5 times**	**More than 5 times**	**Don't have/use**	**Never**	**Only 1 time**	**2-3 times**	**4-5 times**	**More than 5 times**
Social networking site	24 (17)	40 (28)	14 (10)	11 (8)	1 (1)	9 (6)	21 (13)	29 (18)	14 (9)	24 (15)	0 (0)	13 (8)
Instant messenger	33 (23)	44 (31)	6 (4)	10 (7)	3 (2)	4 (3)	29 (18)	29 (18)	15 (9)	11 (7)	5 (3)	10 (6)
Webcam	44 (31)	49 (34)	4 (3)	1 (1)	0 (0)	1 (1)	43 (27)	47 (29)	3 (2)	3 (2)	2 (1)	2 (1)
Mobile phone	33 (23)	37 (26)	11 (8)	14 (10)	0 (0)	4 (3)	33 (21)	35 (22)	9 (6)	6 (4)	8 (5)	8 (5)
Chat room	32 (22)	48 (33)	12 (8)	3 (2)	0 (0)	6 (4)	27 (17)	43 (27)	8 (5)	5 (3)	2 (1)	16 (10)
Blog	49 (34)	46 (32)	1 (1)	3 (2)	0 (0)	1 (1)	52 (33)	35 (22)	3 (2)	2 (1)	3 (2)	5 (3)
Online game	10 (7)	51 (36)	11 (8)	10 (7)	1 (1)	16 (11)	19 (12)	41 (26)	13 (8)	3 (2)	5 (3)	19 (12)
Other	--	0 (0)	1 (1)	1 (1)	0 (0)	0 (0)	91 (65)	6 (4)	1 (1)	0 (0)	0 (0)	1 (1)

Finally, students were asked what action they would take if they were (hypothetically) contacted online by someone they did not know (Table 27). At pre-test, the majority of students reported that should this occur, they would not respond to the messages (11 years: 77%, *n* = 154; 12 years: 79%, *n* = 55), leave the chat session or log out immediately (11 years: 74%, *n* = 147; 12 years: 76%, *n* = 53), block the person who contacted them (11 years: 82%, *n* = 161; 12 years: 83%, *n* = 58), keep the messages as evidence (11 years: 55%, *n* = 107; 12 years: 64%, *n* = 44), talk to a parent about it (11 years: 74%, *n* = 145; 12 years: 76%, *n* = 53), talk to a friend about it (11 years: 66%, *n* = 129; 12 years: 75%, *n* = 50), talk to other family members about it (11 years: 58%, *n* = 114; 12 years: 59%, *n* = 41), set their social networking site profile to private (11 years: 79%, *n* = 153; 12 years: 74%, *n* = 51) and not open the messages or emails sent to them from the person they did not know in person (11 years: 80%, *n* = 156; 12 years: 75%, *n* = 50). Fewer students reported they would talk to a teacher/principal (11 years: 37%, *n* = 72; 12 years: 32%, *n* = 22), talk to the police (11 years: 22%, *n* = 43; 12 years: 24%, *n* = 16), or talk to their Internet Service Provider (11 years: 20%, *n* = 38; 12 years: 11%, *n* = 8) about the contact.[11]

[11] This is one of the areas that I think we can investigate more. I would like to suggest that this is best placed in a journal submission as we can build this from the papers that the CHPRC have had published recently looking at the effects of student actions after victimisation.

Table 27. Likely response if contacted online by someone unknown

	Pre-test % (*n*)				Post-test % (*n*)			
	11 years		12 years		11 years		12 years	
	No	Yes	No	Yes	No	Yes	No	Yes
Not respond to the messages	23 (45)	77 (154)	21 (15)	79 (55)	24 (46)	76 (145)	29 (19)	71 (46)
I would leave the chat session or log out immediately	26 (51)	74 (147)	24 (17)	76 (53)	25 (47)	75 (144)	27 (17)	73 (47)
Block the person who contacted me	18 (35)	82 (161)	17 (12)	83 (58)	14 (27)	86 (163)	21 (13)	79 (50)
Keep the messages/chat as evidence	45 (86)	55 (107)	36 (25)	64 (44)	37 (69)	63 (119)	36 (23)	64 (41)
Talk to a parent about it	26 (52)	74 (145)	24 (17)	76 (53)	29 (55)	71 (136)	32 (21)	68 (44)
Talk to a teacher/principal about it	63 (124)	37 (72)	68 (47)	32 (22)	63 (120)	37 (69)	32 (21)	68 (44)
Talk to the police about it	78 (153)	22 (43)	76 (52)	24 (16)	66 (123)	34 (64)	72 (46)	28 (18)
Talk to a friend about it	34 (66)	66 (129)	25 (17)	75 (50)	28 (54)	72 (136)	27 (17)	73 (46)
Talk to other family members about it	42 (82)	58 (114)	41 (28)	59 (41)	45 (85)	55 (104)	45 (29)	55 (35)
Talk to my Internet Service Provider about it	80 (82)	20 (38)	89 (62)	11 (8)	82 (154)	18 (34)	86 (56)	14 (9)
Talk to someone else about it	90 (138)	10 (16)	89 (47)	11 (6)	78 (95)	22 (26)	71 (30)	29 (12)
Set my social networking profile to private	21 (42)	79 (153)	26 (18)	74 (51)	14 (27)	86 (162)	24 (15)	76 (47)
Make sure I did not open any messages or emails that the person I don't know sent me	20 (39)	80 (156)	25 (17)	75 (50)	18 (34)	82 (153)	27 (17)	73 (6)
Other	96 (200)	4 (9)	99 (70)	1 (1)	96 (201)	4 (8)	99 (70)	1 (1)

Participants' responses to the above question were summed to create a score of positive actions students would take if they were contacted online by someone they did not know in person (Table 28). At pre-test scores ranged from zero to 13 for 11-year-old students and zero to 12 for 12-year-old students. At pre-test, 51% (*n* = 73) of 11-year-old students reported they would do enough actions that classified them as being in the 'average or above category'. The proportion of students classified as this at post-test rose to 60% (*n* = 67). While the actual number of students who reported this decreased, this may be due to

student absenteeism on the post-test data collection date. Figures 11 and 12 below present the actions reported by 11 and 12-year-olds that changed at least 5% from the pre to the post-activity assessments (going either up or down).

Table 28. Score of positive actions students would undertake if contacted by someone they did not know in person

	Pre-test				Post-test			
	11 years		12 years		11 years		12 years	
	%	*n*	%	*n*	%	*n*	%	*n*
Lower than average	48	101	51	36	49	103	59	42
Average or above	52	109	49	35	51	107	41	29

Figure 11. Likely response by 11-year-olds if contacted online by someone unknown

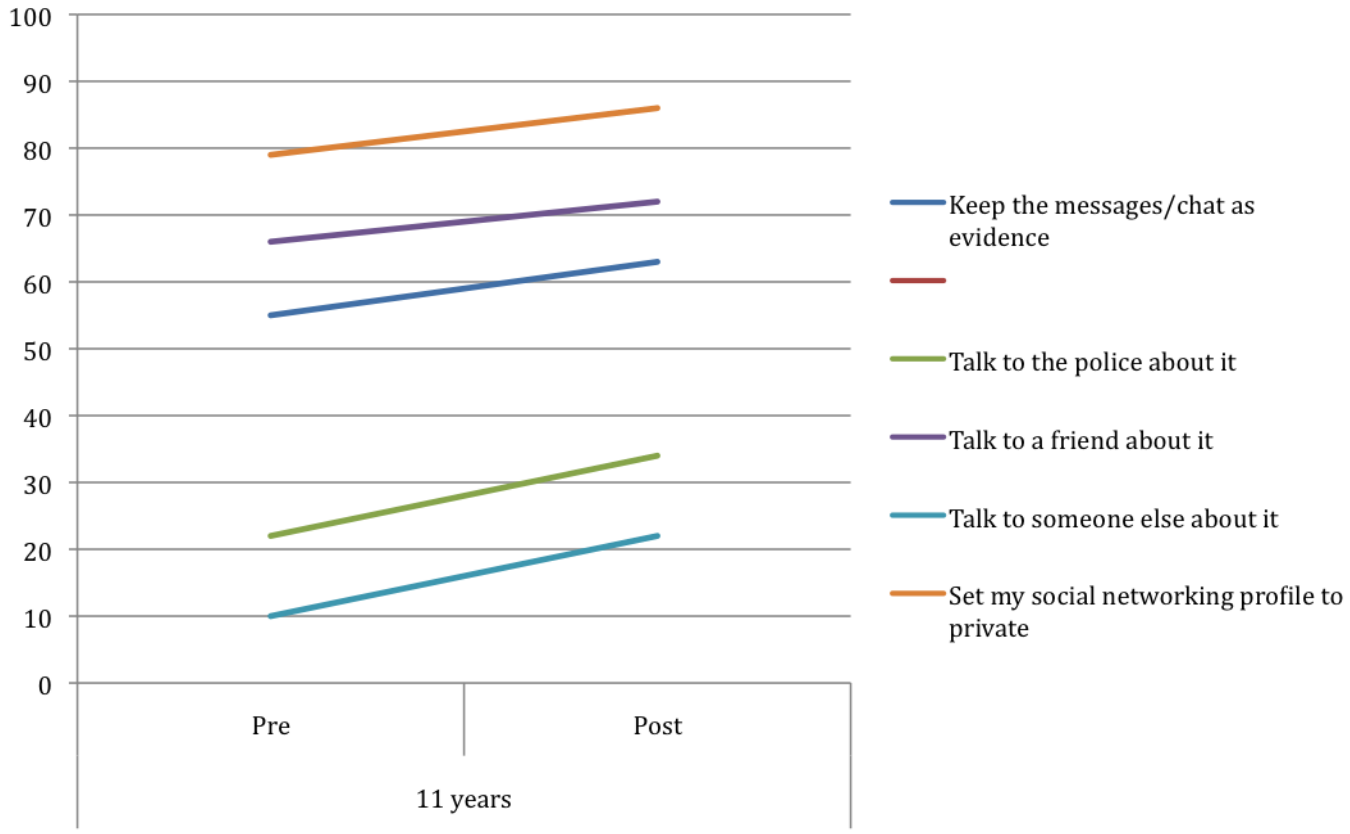
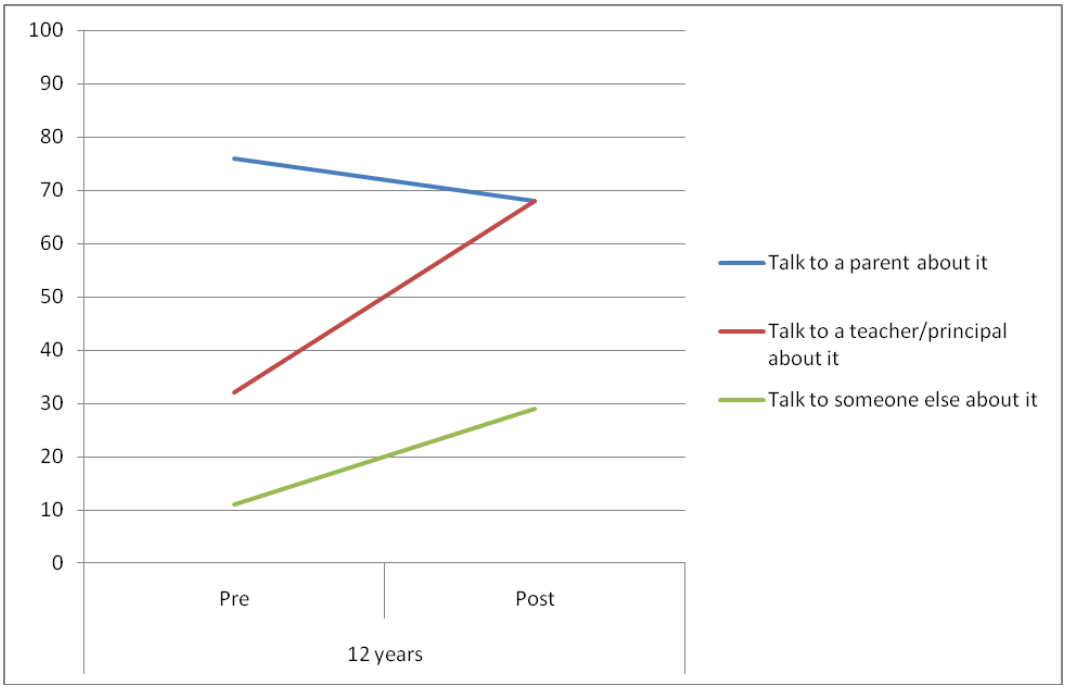


Figure 12. Likely response by 12-year-olds if contacted by someone unknown



Paired (or dependent) t-tests were conducted to determine any significant changes in the number of positive actions students reported they would take if they were contacted online by someone they did not know in person. These data were compared to identify changes in proposed behaviours amongst 11- and 12-year-old students individually, as well as amongst those students who reported a lower than average number of positive actions at baseline. These analyses demonstrate:

- In general, 11-year-old students reported significantly more positive actions at post-test (M = 7.5, SE = 0.2) than at pre-test (M = 6.8, SE = 0.2), $t(193) = -2.946$, $p = 0.004$.

- In general, there was no statistically significant difference between the pre-test and post-test scores of 12-year-old students ($p = 0.914$).

- Amongst the group of students who, at pre-test, reported a lower than average number of positive actions to implement should they be contacted online by someone they do not know in person, pre-test and post-test scores differed significantly. On average, these students' reported positive actions significantly increased from pre-test (M = 4.1, SE = 0.2) to post-test (M = 5.9, SE = 0.2), $t(130) = -5.617$, $p < .001$, $r = 0.072$.

This suggests the CSD activity may be particularly useful for 11-year-students and those students who have lower than average awareness of actions to take (e.g., telling parents, teachers, friends) if contacted online by someone they do not know in person.

4.4.9 CSD activity recall

In the post-test questionnaire, students were asked a series of questions to measure how well they recalled various components of the CSD activity as part of assessing the extent to which content and messages presented in the activity. This section presents the results of the eight questions relating to students' recollection of the game (Table 29). It is important to note that these items were presented in a multiple-choice format. First, students were asked to recall the age of the girl (Sarah) in the story. Almost half of 11-year-old students recalled the age of the girl in the story correctly, being 13 years (47%, *n* = 90), while 38% (*n* = 25) of 12-year-old students could not correctly recall this fact. Students were next asked to recall who had been contacting Sarah. Almost all students answered this question correctly with the response 'Kel17' (11 years: 94%, *n* = 183; 12 years: 95%, *n* = 62). The majority of students were able to recall Sarah's hobby as rollerblading (11 years: 88%, *n* = 171; 12 years: 90%, *n* = 57).

The majority of students recalled that the boy got Sarah's mobile number online (11 years: 81%, *n* = 157; 12 years: 78%, *n* = 51). In the story, the boy wanted to take Sarah to the skate park. Almost all students answered this question correctly (11 years: 90%, *n* = 174; 12 years: 86%, *n* = 56). Students were able to recall the location of Sarah's computer at home quite well with 87% (*n* = 168) of 11-year-old and 83% (*n* = 54) of 12-year-old students reporting the computer was located in her bedroom. Towards the end of the scenario, students found out the person waiting to meet Sarah was 37 years old. More 11 (67%, *n* = 129) than 12 (58%, *n* = 38) year old students answered this question correctly. Finally, students were asked to recall whether police were called in the story. While 12% (*n* = 23) of 11-year-old and 15% (*n* = 10) of 12-year-old students could not remember if this occurred, 79% (*n* = 153) and 71% (*n* = 46) of 11- and 12-year-old students (respectively) answered correctly that the police had been called.

Table 29. Students' recall of components of CSD script

		11 years		12 years	
		%	*n*	%	*n*
Age of girl in story (Sarah)	I don't remember	22	42	38	25
	13 years	47	90	32	21
	14 years	19	37	8	5
	15 years	11	22	21	14
Person contacting Sarah	I don't remember	3	6	1	1
	Tel 15	1	1	1	1
	Kel17	94	183	95	62
	Tim16	2	4	1	1
Sarah's hobby	I don't remember	8	15	8	5
	Rollerblading	88	171	90	57
	Biking	3	6	2	1
	Running	1	2	0	0
How boy got Sarah's mobile phone number	I don't remember	11	21	11	7
	She gave it to him	7	14	11	7
	They had friends in common	1	1	0	0
	He got it online	81	157	78	51
Where the boy wanted to take Sarah	I don't remember	6	12	8	5
	His house	4	7	5	3
	Local skate park	90	174	86	56
	To the cinema	0	0	1	1
Location of Sarah's home computer	I don't remember	11	22	12	8
	In her bedroom	87	168	83	54
	In the family room	1	3	1	1
	She does not have one at home	1	1	3	2
Age of person waiting to meet Sarah	I don't remember	11	21	17	11
	17 years	15	30	14	9
	37 years	67	129	58	38
	21 years	7	14	11	7
Police contacted in story	I don't remember	12	23	15	10
	Yes	79	153	71	46
	No	9	17	14	9

4.4.10 Results by risk level

At pre- and post-test, students were provided a list of actions they could take if approached online by someone unknown to them. The number of actions students reported they would do was summed to create an 'action score'.

At pre-test, the mean action score was 6.81 (standard deviation [sd] = 3.29). Students were classified as being at high-risk (*n* = 60), if their action score was greater than one standard deviation below the mean (i.e., reported taking fewer actions). Using rounded values, an action score of four or lower classified students as being at high-risk. Students were classified as being at low risk (*n* = 54) if their action score was greater than one standard deviation above the mean. Thus, students with an action score of 10 or higher were classified as low risk (i.e., reported taking more actions). Students with a score between 5 and 9 were classified as having moderate risk. Slightly more 11 year old (54%) than 12 year old (46%) students were classified as being at high-risk at pre-test; however, at post-test, this trend was reversed, with slightly more 12 year old (58%) than 11 year old (48%) students being identified in the high-risk category.

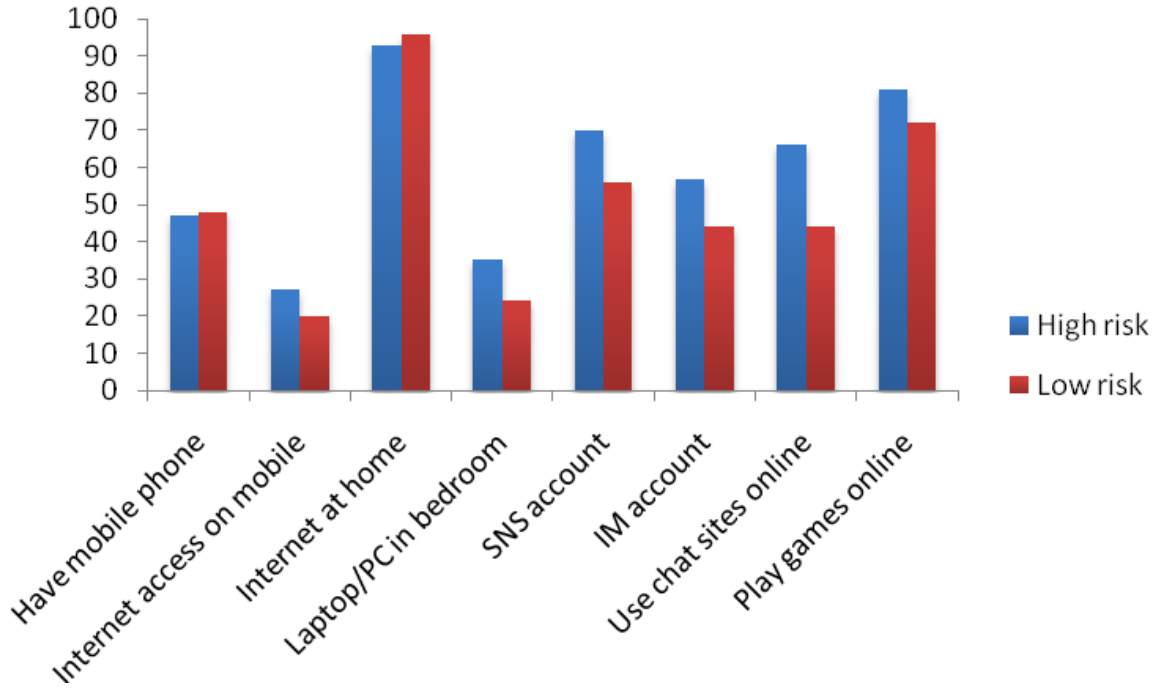
Technology use:

- While the frequency of phone calls made and received on mobile phones was similar across risk groups, high-risk students (9%) reported sending a higher number (6-10) of text messages on their mobile phone on an average day at school compared to low risk students (2%).
- When asked how many times on an average school day they used the Internet on their mobile phone, low risk students (11%) more frequently stated doing so one to three times per day, than high-risk students (5%).
- High-risk students did, however, report higher use rates (Internet on their mobile phone) on an average day of the weekend. High-risk students (versus low-risk students) more frequently reported doing so one to three times per day (15% versus 9%), four to five times per day (5% versus 4%) and more than 10 times per day (5% versus 0%); while 6% of low-risk compared to 2% of high-risk students reported using the Internet on their mobile phone between six and 10 times per day on the weekend.
- While the proportion of students in both risk groups who reported using the Internet for school work on an average week day was similar, high-risk students reported more

weekday use of the Internet not for school week, compared to low-risk students (e.g., about three hours/day – high: 10%; low: 4%).

- More low-risk students (41%) used the Internet on an average day of the weekend for about 1 hour for school work compared to high-risk students (15%), and also for about two hours (15% compared to 7%), while use at higher levels was similar across both groups. Lower level use was higher in the high-risk group (57% reported using the Internet for school work for less than one hour on the weekend), compared to low-risk students (30%).
- High-risk students again had higher weekend use of the Internet, not for school work; 7% of high-risk students used the Internet for about four hours on the weekend not for school work, compared to 0% of low-risk students and 20% of high-risk students used the Internet for more than four hours for the same purpose, compared to 4% of low-risk students.
- A similar percentage of students in both risk groups used the Internet at home (High: 88%; Low: 94%) and slightly more low-risk students reported using the Internet at school (High: 37%; Low: 55%).
- When at home, 48% of high-risk and 59% of low-risk students reported they usually use the Internet in an open area and 50% and 44% (respectively) reported using the Internet in the study or separate room; while 22% of students in both risk groups reported using the Internet in their bedroom.
- More high-risk (73%) compared to low-risk (59%) reported having a social networking site or instant messenger and their use of this site was higher when compared to low-risk students (for example, when asked about before/after school use, 7% of high-risk students reported using this site for about an hour compared to 4% of low-risk students, and 7% reported use for about two hours, compared to 4% of low-risk students).
- Two-thirds of high-risk (66%) compared to just less than half of low-risk (44%) students reported they use chat sites on the Internet.
- A similar portion of students in both risk groups reported playing games on the Internet (High: 81%; Low: 72%); however, more low-risk students (35%) reported they play online games that don't involve other people compared to high-risk students (14%) and more high-risk (49%) compared to low-risk (16%) students reported playing online games with both people they know and those they have never met.

Figure 13. Technology use by risk group

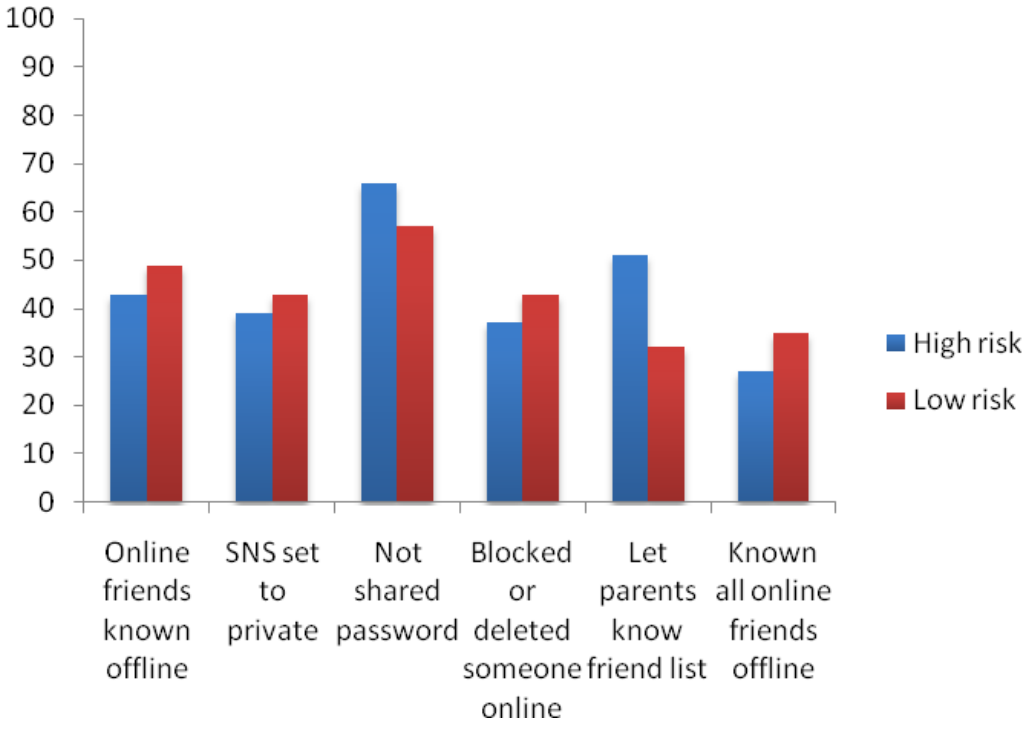


Online interaction:

- Just under half of students (High: 43%; Low: 49%) reported they only have friends online that they have met in person.
- Approximately two-thirds (High: 39%; Low: 43%) of students reported they have set their social networking profile to private.
- Two-thirds of students reported they have not shared their password with anyone (High: 66%; Low: 57%).
- Two-thirds of students (High: 37%; Low: 43%) reported having blocked or deleted someone who said something rude or mean.
- More low-risk (51%) than high-risk (32%) students reported they let their parents know who is on their friends list.
- About one-third of students (High: 27%; Low: 35%) reported knowing 'all' of their online friends in person and a further one-third of high (30%) risk students reported knowing 'nearly all' of their online friends in person, while only 9% of low-risk students knew 'nearly all' of their online friends.

There were several differences between the high-risk and low-risk group in relation to online contact by unknown persons (percent of students who reported this had occurred at least once).

Figure 14. Online interaction factors by risk group



Actions taken if contacted online by unknown person:

- More high-risk, but fewer low-risk students reported they would not respond to messages at post-test than at pre-test (High: 35% to 48%; Low: 98% to 81%).
- More high-risk students reported they would leave the chat session or log out immediately at post-test compared to pre-test (13% to 48%) and fewer low-risk students reported this at post-test (100% to 80%).
- More high-risk students reported this action at post-test (28% to 60%) and fewer low-risk students reported (100% to 87%) they would block the person who contacted them.
- Keep the messages/chat as evidence: More high-risk (20% to 53%) and fewer low-risk (89% to 78%) students reported this at post-test than pre-test.
- Talk to a parent about it: More high-risk (13% to 38%) but fewer low-risk (100% to 85%) students reported this action between pre- and post-tests.
- Talk to a teacher/principal about it: More high-risk (2% to 23%) but fewer low-risk (89% to 65%) students reported this action from pre- to post-tests.
- Talk to the police about it: More high-risk (0% to 27%) and fewer low-risk (74% to 59%) students reported this action at post-test than pre-test.
- Talk to a friend about it: More high-risk (30% to 62%) but fewer low-risk (80% to 68%) students reported they would take this action.
- Talk to other family members about it: More high-risk (13% to 37%) and fewer low-risk (81% to 65%) students reported this action.
- Talk to my Internet Service Provider about it: More high-risk (0% to 13%) but fewer low-risk (56% to 31%) students reported they would take this action.
- Talk to someone else about it: More high-risk (0% to 17%) and a similar proportion of low-risk (28% to 24%) students reported they would take this action.
- More high-risk (15% to 48%) but fewer low-risk (100% to 87%) students reported they would set their social networking profile to private.
- More high-risk (23% to 48%) but fewer low-risk (98% to 85%) students reported they would not open any messages or emails from a person they did know.

Figure 15. Actions taken by high-risk group if contacted online by unknown person

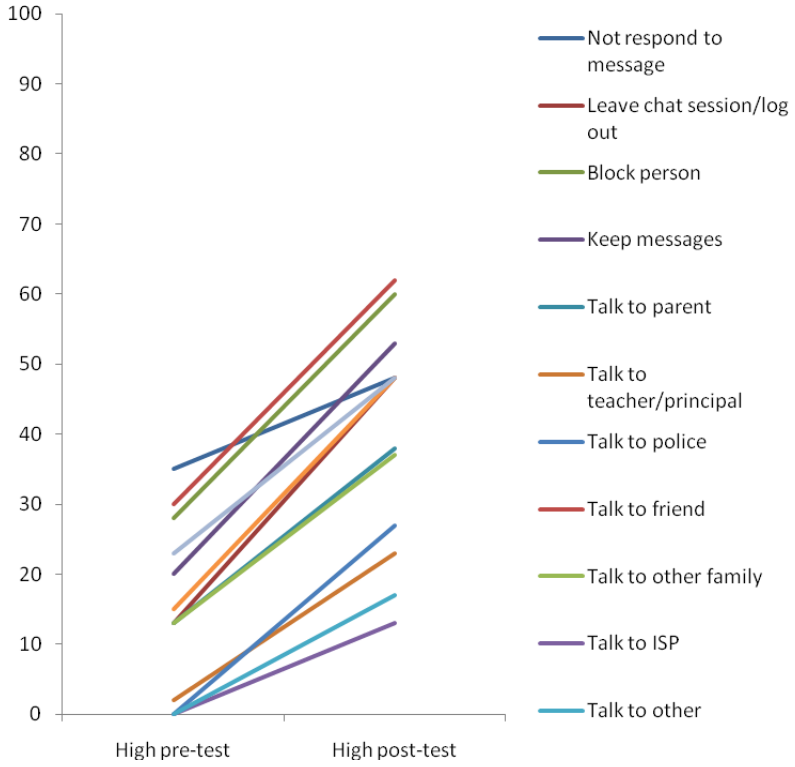
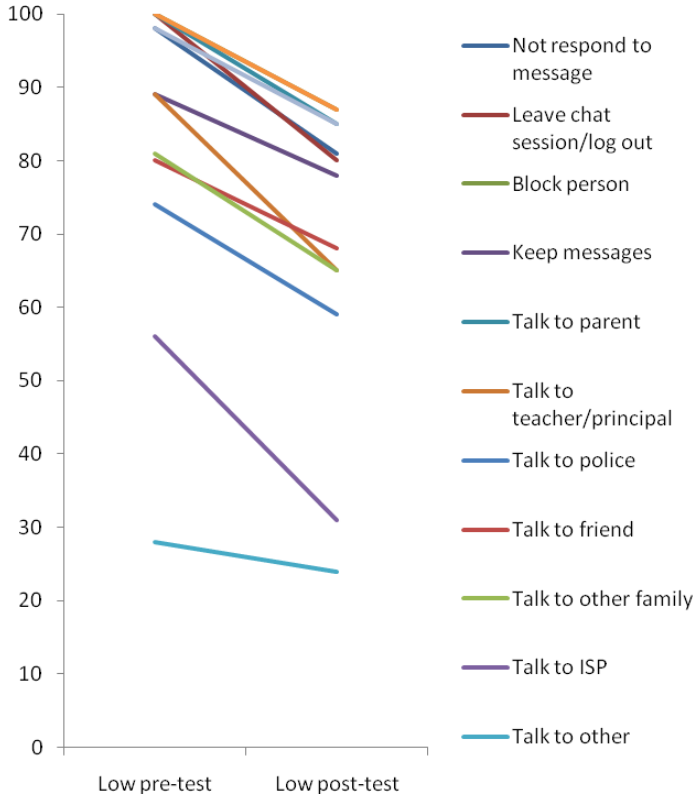


Figure 16. Actions taken by low-risk group if contacted online by unknown person



4.4.11 Comparison by risk level

Some important results were found in relation to the risk group differences between the pre and post-test assessments. Overall, high-risk students reported significantly more positive actions at post-test (M = 5.4, SE = 3.56) than at pre-test (M = 1.85, SE = 1.67), t(60) = -6.334, p < 0.001. Hence, students classified at pre-test as being high-risk were less likely to be classified as such at post-test. Furthermore, low-risk students reported significantly fewer positive actions at post-test (M = 10.92, SE = 0.87) than pre-test (M = 9.7, SE = 2.47), t(50) = 3.464, p = 0.001. However, in reality, this difference is quite low and, importantly, did not result in a change to their risk status.

4.5 Student qualitative results

The following presents a summary of student responses to questions asked during focus groups for the evaluation of Cybersmart Detectives (CSD). Each question asked is highlighted and an overall summary of the responses across participants is described with each major theme highlighted as bold text. Further, a table highlighting the major themes identified for each question is presented, including an indication of the number of times each is referenced by respondents.

A total of sixteen focus groups were successfully completed with students from seven schools. Focus groups were delineated by gender, with eight being conducted with females and six with males. Two focus groups were completed with both male and female participants due to an insufficient number of male students present on the day. In total, 87 students, 49 female and 38 male students, participated in the 18 focus groups.

While tables have been provided to indicate strength of all recurrent themes; they are not a standard way of presenting qualitative findings. The main themes have been written as a qualitative summary and are discussed in text using the terms 'majority', 'most', 'many', 'some' and 'a few'. Each of these categories are based on the number of references and sources of information following the thematic coding process. Supporting quotes are presented with the school pseudonym (school ID), followed by gender of the focus group (F = female, M = male, FM = combined male and female group). For example, the ID "Scl_008_M" would refer to a male focus group from school number eight while "Scl_012_FM" would refer to a combined male and female group from school twelve. The supporting quotes (both positive and negative) are provided to highlight CSD activity strengths and suggestions for improvement.

4.5.1 Initial impressions of CSD activity

The majority of respondents who made comments regarding their initial impressions of the game suggested CSD activity was **not what they expected** it to be, "it was way funner! [**fun**]":

> *"It was different to what we expected a game to be – it was way better, because you get involved in it more than with other games. This one [Cybersmart Detectives] was more like email, like what we usually do [use]."* [Scl_004_F]

Further, another student commented:

*"the game was really more about educating [**educational**] what we should do online but in a fun way and being able to solve problems [**problem solving**]."* [Scl_001_M]

> *"It was sort of good when they give you something and then you had to think it through. You write down your answer and it makes you think you're actually in a real case."*
>
> [Scl_001_M]

Many students indicated they felt the game scenario provided an **easy to understand**, interesting and engaging storyline. Student commentary also suggested that many students related to the CSD activity characters and were able to envisage the scenario occurring at their school:

> *"It was a very good storyline – I enjoyed how someone found the phone and you had to try and track it to who it belonged to. It kind of showed a 'moral of the story' kind of thing – like keeping your profile private and not going [meeting up] with just anyone."* [Scl_007_M]

4.5.2 Game enjoyment

Respondents were asked to contemplate if they enjoyed playing the CSD activity. The majority of respondents in thirteen focus groups **unanimously** indicated they enjoyed playing the CSD activity, with a **mixed response** in three of the focus groups as some students enjoyed the game while others in the same class did not. Respondents from two focus groups; one male focus group and one female focus group (both from the same school) indicated they did not enjoy playing the game.

When asked why they enjoyed playing the CSD activity, the majority of respondents acknowledged they liked **answering questions** and **receiving feedback** (Table 30). Further, most respondents enjoyed the **interactive** functionality of the CSD activity and made positive comments regarding their ability to *"send something and get an immediate response"* (**communicate with others in real time**). A few respondents also suggested they appreciated the ability to work in a team (**teamwork**) as a means to consolidate their ideas and feel confident **voicing their thoughts and opinions** regarding solutions to the CSD activity scenario:

> *"I enjoyed writing and getting something back, like it was really cool to interact with someone else."* [Scl_007_M]

"You could send messages to people and you actually get a response… yeah, getting a response is good - responses to questions that you asked, so I felt that someone was really listening to what we had to say. The messages [feedback from the control room and guides] are a really important part of the game." [Scl_004_F]

"Being able to make your own decisions, actually say what you believe in and discuss that with your partner."
[Scl_004_F]

"I really liked that we could communicate with other people and we really, like, became a team. To be able to work in a team on that game was really, really fun." [Scl_001_M]

Many respondents also commented they found the game **interesting** and **enjoyable** as the scenario was **realistic** and *"it felt like I was a detective"* [Schl_005_M] (**felt like investigative / detective work)** as it included unexpected elements of mystery and discovery, therefore *"you didn't know what to expect"*:

"If we were ever in that situation we would know what to do as it [the CSD activity] was based on something that could actually happen to you." [Scl_004_F]

"I liked the fact that it was a real life situation – it was as if you were dealing with real people and could get advice from real people." [Scl_007_F]

"I liked the mystery, so trying to discover something was quite fun… I liked being a detective and figuring out what happened, figuring out all the clues and then putting them all together." [Scl_005_F]

Many students also indicated the **poll questions** added to their enjoyment of the CSD activity as the questions highlighted important learning opportunities (**opportunity to learn something new**) throughout the game. Further, students mentioned they also enjoyed finding out how many respondents answered the same as they did:

"Getting answers and seeing what other people thought – the poll questions really helped you think about what you had learnt… about how to be safer online." [Scl_012_FM]

"I quite enjoyed the polls, when you send questions and there were a few multiple choice – I found those quite fun. I like seeing how many people gave responses to the answers."

[Scl_007_M]

"It [Cybersmart Detectives] was probably my favourite online educational game that I have actually played. I felt like I was learning what to do in certain situations and if I was getting texted by someone on my phone, I would know what to do." [Scl_005_M]

Two respondents commented they enjoyed playing the game as it gave them an opportunity to *"**do something you haven't done before** (i.e. using a chat site)"* [Schl_005_M]:

"I don't have a chat room [as] my mum doesn't like it… [so] I have never been on a site where you get to interact with people so quickly… cause I don't usually have [access to] that." [Scl_001_M]

Table 30. Elements of the Cybersmart Detectives game respondents indicated they enjoyed

Things respondents enjoyed about the game:	*n*
Answering questions, and receiving feedback	21
Felt like investigative/ detective work (mystery, discovery)	15
Interactive	12
Real time communication	11
Realistic	11
Poll questions	10
Enjoyable	7
Interesting	7
Ability voice thoughts and opinions	6
The opportunity to learn something new	5
Teamwork	3
Doing something you haven't done before (i.e. using a chat site)	2

Respondents were then asked to contemplate elements of the CSD activity they did not enjoy or disliked (Table 31). The majority of students acknowledged they found **some of the questions difficult or confusing to answer**. This feeling was compounded by a **lack of understanding as to how to play the game**; a sentiment which subsided after students read the guide book (if provided to them by the class teacher) or alternatively persisted with the game, as "once you've sussed it out its gets easier as you go along" [Scl_010_M]:

"If you miss one question and get it wrong you get a bit lost as you don't know what to do… but the game keeps going on." [Scl_005_F]

"It got a bit confusing that there were grey, green and purple messages – we got confused as to which one was important and just started clicking them all." [Scl_004_F]

"At the beginning, I got a bit confused. I needed a bit more information on how to play the game. Like, the one where we had to search her name [as we did not realise it was not an active link] – that one confused me as I was not sure if I actually had to search her name or not. It got easier to understand after two or three questions." [Scl_007_M]

Many students also commented they felt there was an inappropriate amount of time between scenario messages sent from control room, suggesting "*they came through **too slow***":

"It wasn't quick… we just waited a long time - It sort of went on forever. I felt that whenever you typed it in and sent it [a message] you would have to wait and then he'd [control room] reply and then you would reply back to him [control room] and then you'd have to wait another five minutes or something [to receive another message]." [Scl_001_M]

Conversely, other students commented the length of time between scenario messages sent from the control room was too fast:

"You'd type a big paragraph and then you send it and then you look back on your message screen and you've got three things you have to click open… after that there is just more and more and you don't have enough time to read them all." [Scl_001_M]

When messages were delivered too fast, many students also indicated they were confused regarding the **sequence of messages and/or responses**:

"All of the messages came at once and it is a bit like 'what one do we read first, oh, is there supposed to be some order and will it make sense if we read it out of order?' I didn't get that either." [Scl_012_FM]

"Our group didn't know if we had to answer every single question because they came up at different times – you might be answering a question and two more pop up… when the teacher replied to us and said 'what next', we had to try and find which

questions the answer was for – that was confusing… it was a little bit hard to know what question you were up to." [Scl_007_M]

"We didn't really get at first what we had to reply to [blue questions], but then halfway through the game we finally got it – because we didn't see those questions before – so I think they [blue questions] should have been positioned closer to the story part."

[Scl_004_F]

Students also commented on instances when upon responding to one message sent from the control room they would return to their inbox and find too many messages; further, as the game progressed they retained **too many messages in their inbox** resulting in a cluttered screen:

"When you are reading and responding to a message, another one pops up, then all of a sudden you have five messages [unread in your inbox] and you lose track of where you are at." [Scl_005_M]

"We didn't know if our inbox would get full and were trying to delete some of the messages so we could see the new messages only." [Scl_005_M]

Some respondents were also unaware as to the location of game function buttons (**could not find game function buttons**) (i.e., send message button), which initially hindered their progression through and understanding of the CSD activity:

"At the beginning we got a bit confused because there was not a 'reply' button, you had to click 'send message' to reply to a message that you had clicked on – and that was a bit like 'why isn't there just a reply button?" [Scl_004_F]

A few respondents suggested the game duration was too long (**game-play too long**). However, many of these respondents indicated the CSD activity should not be shortened as this length of time allowed for students to *"get used to the game"*:

"It took a long time. Did it take about an hour and a half? It dragged on a little bit."

[Scl_004_F]

A few students also commented they received an **inappropriate response to their question/s,** indicating they *"got the same answers back a couple of times"*, suggesting they felt the comments were *"cut and paste"* [Scl_001_M]. Further students also noted instances

where the **response time to student questions was too slow** suggesting the "messages were like snail mail" (i.e., they had to wait too long to receive a response to their question/s):

> *"At certain points in the game I found it going really slow… we were just sitting there waiting for the next one."* [Scl_005_M]

Only a few students commented they felt the game was **boring**, **simplistic** (i.e., just writing), or **did not feel like investigative/detective work** as

"we didn't really solve any of the problems… we sort of just gave answers... I don't feel like we really solved anything" [Scl_010_F].

Conversely, students in one focus group expressed they enjoyed everything about the game (i.e. disliked **nothing**). Interestingly, student participants from two focus groups reported that they felt the game sent **contradictory** cyber-safety messages as students did not know who was in the control room; however, were required to communicate with them as part of the game:

> *"It felt a bit weird as the game was telling you not to talk to people you don't know, but you are actually talking to people you don't know!"* [Scl_005_M]

> *"The game is all about 'don't speak to people you don't really know [our team] were saying, 'well, we really don't know these people [in the control room]'. Yeah, we were emailing [Control room person 1] and [Control room person 2] and asking ourselves 'who are these people? We don't really know!"* [Scl_004_F]

Table 31. Elements of the Cybersmart Detectives game respondents indicated they did not enjoy

Things respondents did not enjoy about the game:	*n*
Some questions were difficult to answer/ confusing	14
Did not understand how to play the game at first (only easy to understand after a while)	13
Inappropriate time between scenario messages sent from control room – too slow	12
Not understanding sequence of messages / responses	9
Could not find game function buttons (i.e., send message)	6
Game play too long	6
Inappropriate time between scenario messages sent from control room – too fast	6
Inappropriate response to student questions	5
It was boring	5
Game play too simplistic (i.e., just writing)	4
Inappropriate response time to student questions – too slow	4
Too many messages in inbox (cluttered screen)	4
Did not feel like investigative/ detective work	2
Game was contradictory as students did not know who was on the control room yet were communicating with them	2
Nothing	1

4.5.3 Cyber-safety awareness

Respondents were then asked to consider the ways in which the game made them think about cyber-safety and how to be safer online (Table 32). The majority of respondents indicated the game reinforced that when online, individuals should **not communicate with people they do not know face-to-face**:

> *"I think I will be more careful on sites that have anything to do with messaging and if anyone messages me, like strangers I don't know, I think I would just ignore or probably delete them."* [Scl_007_M]

> *"It's important to know who you are talking to… ignore messages from people you don't know."* [Scl_006_F]

As a means to limit who has access to them online, students indicated the need to **set your SNS profile to private**:

"Being safe on the Internet and having private stuff [setting your profile to private] so people can't just go in and randomly, like Kel, tricking you for your ID and stuff." [Scl_010_M]

Notably, a few students disclosed that prior to playing the game, they had been unaware of **the existence of privacy setting controls on SNS**, indicating the game was a useful medium to communicate that users are responsible for and have control over SNS privacy settings:

"*I now know you can set your profile to private… like on Facebook, they make it really hard to find the privacy settings so how would you ever know... they hide it."*

[Scl_001_M]

Many students also suggested they would **limit who can access their SNS profile to friends and family they know face-to-face** and **only 'accept' online friends they also know face-to-face**:

"You should always have MySpace, MSN and any of those things set on private, so only your friends and family can see it." [Scl_012_MF]

"*Only add people [to your SNS profile page] that you know from school… don't just add people as friends because they look cool."* [Scl_005_M]

Some respondents also acknowledged that the CSD activity highlighted the concept of *"stranger danger"* as **it is easy for others to conceal their real identity when online**. Many also touched on the potential risks associated with meeting up with someone face-to-face you met online [**do not meet people face-to-face you only know online**]; hence indicating they would never do so:

"*Even if you did have privacy settings and stuff, you should only meet up with people [face-to-face] you know."* [Scl_012_MF]

"Just because you think you know them, because you have been talking to them on the Internet, doesn't mean they are who they say they are… people can lie online, they don't have to tell the exact truth."

[Scl_010_F]

A few respondents suggested they would be more **mindful of the SNS they subscribe to** (i.e., ensure they only subscribe to age appropriate websites[12]) and would **not share their passwords with others**, even their close friends:

"*You should delete your account on Facebook, as we are not over 18 anyway and try to use MSN, because over MSN, you don't have any requirements for your age."* [Scl_001_M]

Further, students were asked to consider what changes they would make, if any, to the websites they currently visit and the type of information they post online. The majority of respondents suggested they would **limit, remove or refrain from posting personal information online**:

"You should not put so much personal information online. If you give away your school, people can find you." [Scl_012_FM]

"I have my birth date on my Facebook profile – I will take that down." [Scl_005_F]

A few respondents also acknowledged they would ensure they **did not post personal information about other people online**:

"You should probably not say anything about your friends either because sometimes for some things you can say things about your friends and other people can find out about them… yeah, other people can read the wall [i.e. profile page]." [Scl_012_MF]

"Don't put up photos of other people without asking them." [Scl_005_F]

Respondents continued to discuss what they would do should they be contacted online by someone they do not know. Depending on the circumstance, the majority of respondents indicated they would **seek advice from friends, parents and/or police when necessary**:

"Before this [game] I never thought it would be a police matter, I would have just thought to ask a parent or teacher for help with these sorts of things, but after we have done this [game] I have realised that it can go into a police matter the further it goes on."

[Scl_012_MF]

[12] Facebook Terms and Conditions state users must not be under 13 years of age: http://www.facebook.com/terms.php?ref=pf

Many also suggested they would **allow their parents to access their SNS profile and/or check websites they visit** to ensure only legitimate and safe contact was made when communicating online. One student added they only use secure Internet sites to ensure they safely access appropriate content (**look for secure sites**) when searching for information. Further, to assist parental monitoring a few students noted they would ensure their computer was located in a communal family area rather than in their bedroom (**no computer in bedroom**):

> *"You should probably let parents supervise you when you are on the Internet… to make sure your parents actually know what you are doing."* [Scl_007_F]

A few students indicated **they would not or do not visit these types of sites** and consequently felt they **did not learn anything** or **would not change anything** as a consequence of playing the CSD activity:

> *"I didn't really learn anything new from the game – I already knew all that stuff."*
>
> [Scl_010_F]

Table 32. Cyber-safety messages provoked by the CSD activity

Cyber-safety messages provoked by the CSD activity	*n*
Limit/remove or do not post personal information online	30
Do not communicate with people online you don't know face-to-face	24
Set your SNS to private	14
Limit who can access your SNS profile to friends you know face-to-face and family	11
Seek advice from friends, parents and/or police when necessary	10
The existence of privacy settings on SNS (i.e. there ARE privacy settings)	10
Allow parents to access your SNS profile and/ or check websites you visit	9
Only have online friends you also know face-to-face	9
Do not meet people face-to-face you only know online	8
It is easy for others to conceal their identity online	7
Do not post information about other people online	5
Be mindful of the SNS you subscribe to (i.e. age appropriate)	4
Do not share your password	4
I don't/ won't visit these types of sites	2
No computer in bedroom	2
I did not learn anything	1
I will not change anything	1
Look for secure sites	1

4.5.4 Online educational cyber-safety games

Respondents were asked to think about what they consider to be essential components of an educational cyber-safety game (Table 33). The majority of students suggested the game should be **interactive** and revolve around a **realistic** scenario:

> *"I want to be able to ask the people who are online questions… I would be interested to find out if [the scenario] was a real case and what their answer would have been."*
>
> [Scl_012_FM]

Further, many respondents also commented the game should integrate a **rewards or points scheme in recognition for correct answers** provided by players and/or teams throughout the game; essentially the team *"that comes up with the safest storyline wins"* [Scl_007_M]. This component was also seen as a means to integrate competition into the

game play, as respondents suggested they should only be able to proceed through the game once they have provided an appropriate or correct answer:

> *"For each of the questions you could have to find the correct answer to move on and get to the end."* [Scl_001_M]

Many respondents also commented they would find value in being able to **choose from a variety of different scenarios from a range of topics** as a means to tailor the game to their interest or needs. Notably, one student recalled his experience of being cyber bullied and indicated he would have benefited from a game such as CSD to educate himself and his friends on how to best manage the bullying situation. Some students also noted the **scenarios should be age appropriate** to ensure there was a game suitable for all year levels:

> *"Maybe the website should be that you pick more games to play, more stories and then learn more."* [Scl_012_MF]

> *"I know that younger people sometimes might go on this website to learn, so maybe you should put in age setting, so like, Year 1 might be a bit simpler, like you are on the school email and you learn you don't do this and that."* [Scl_012_MF]

Some respondents made comments regarding the game appearance, mentioning they would like to *"get out of the email box"* to **explore the game environment**. This indicates students would enjoy moving around the virtual space (e.g., schoolyard) using an interactive avatar:

> *"You could be the person finding the phone and the story plays out the same, but you see the actions on the computer screen like a game. I would like to move about."* [Scl_005_F]

> *"Make it active, like you're in it. You need to actually walk around the school yard and discover stuff."* [Scl_005_F]

Further, some students also suggested the game should use **teamwork** and **integrate the use of detective tools** (i.e. a spy phone) as a means to engage users into the game play:

> *"We want to be able to resolve the problem as a team."* [Scl_004_F]

"The younger kids might really want to be a detective and it could be made to look like you actually are a detective, using the tools that detectives use… Instead of clicking on something that says 'send message' you could click on a spy-phone to make it more fun." [Scl_001_M]

A few respondents also suggested an educational game could utilise the '**choose your own adventure**' layout, whereby student's answers to the problem (**needs to solve a problem**) dictate the storyline. This format indicates students believe the user should have greater control and influence over how the game is played out:

"At the start you could have different types of storylines, so you can choose your team and then it asks you 'would you like… which theme would you like – cyber bullying, normal bullying' and then you could play the game more than once, like a choose your own adventure story." [Scl_007_M]

The aforementioned commentary indicates respondents enjoy being challenged (**needs to be challenging**) and appreciate opportunities to use different strategies and methods of navigation to play the game.

Table 33. Essential components of an education cyber-safety game as suggested by respondents

Essential components of an education cyber-safety game as suggested by respondents	n
Needs to be interactive	11
Rewards / points in recognition of correct answers	10
Choice of different scenarios from a range of topics	8
Needs to be realistic	8
To be able to explore the game environment	7
Age appropriate scenarios	6
Needs to use teamwork	6
'Choose your own adventure' style of game play	5
Integrate detective tools (i.e. spy phone) into game play	5
Need to solve a problem	4
Needs to be challenging	3

4.5.5 Cybersmart Detectives game recommendations

The majority of participants commented they would like **more visuals** (pictures and animations) integrated into the game play to maintain interest:

> *"The [CSD] game was just writing. There weren't that many pictures and stuff. Yeah, there should have been more pictures."* [Scl_005_F]

Many also noted they would have valued **clear instructions** prior to playing the game to ensure they have apparent goals and rules regarding their involvement and how to progress through the game (Table 34). *[It is important to note that many participating evaluation schools did not utilise available ACMA resources to prepare their students for game play]:*

> *"When you log on there should be a box that shows you how to play the game – just a little bit about it… or [when you are playing the game and are not sure what to do] there could be an info button, so that when you pressed it, you got information about that bit – so it was just what you needed to know for that particular thing."* [Scl_012_MF]

Many also indicated they would enjoy the opportunity to **communicate with other teams in their class during game play** so they could pose questions and formulate a response based on class members' feedback or suggestions:

> *"If you don't get it [the scenario], it would be good to be able to speak with others in the class to help figure it out. You could do it as a class and all vote on the right option to choose."* [Scl_005_F]

Students also mentioned they would like the game to have a **delete button for all read messages** in order to manually de-clutter the inbox.

> *"[It would be good to have] a delete button, so you know what you have done and what you still need to do – like a real inbox."* [Scl_012_MF]

> *"Try and make it a bit clearer on the screen… don't show all the messages that you have already seen cause it gets confusing."* [Scl_010_M]

Some students also voiced their preference for **working in teams of two rather than a group of three** as it was felt the third person's role was redundant. Alternatively, students suggested all team members should regularly switch roles so each had an

opportunity to take charge of the various responsibilities. A few students even mentioned a preference for **working through the game individually**:

> *"I thought there wasn't enough space around the computer because there were three people in a group and you are crowded around one computer and you can't really see what is going on, so I think working in pairs would be better… Yeah, I was glad I was in a group of only two people, because I was picturing myself in a group of three and it would be chaos."* [Scl_005_M]

> *"We worked in groups of two [and thought it worked well] otherwise, somebody [the third person in the group] doesn't really have something to do."* [Scl_004_F]

Some students noted they would have liked the game interface to read as if they were participating in an instant messenger chat (MSN) rather than email so the game felt more conversational (**messages as a conversation rather than email**).

> *"I would do it so when you are messaging it's more like MSN – and then maybe you could share information with other teams."* [Scl_012_FM]

> *"The inbox is a bit like an email, like you have mail. Maybe you could put it on chat so you could see the conversations as they happen. In a chat room it is easier [to have discussions]."* [Scl_001_M]

Further, one student also indicated this format would be more appropriate given students of their age use MSN more frequently than email. Students also suggested they would like to see who they were communicating with and would like the opportunity to **speak rather than type their responses** (i.e. using a webcam)

> *"Instead of typing [responses] in, I would have a voice transmitter that you could talk to them [control room] and they could actually talk to you."* [Scl_001_M]

One student commented they would like **messages from the control room to arrive in students' inbox at the same time** (simultaneous message delivery), as they felt the game was playing out at different times throughout the various teams in their class:

"When someone got a message across the classroom, it sort of got spoilt because you knew it was coming, it would be good if they [messages] went all exactly the same."

[Scl_012_MF]

Another suggested the game should allow users to **choose the gender of the main characters**, while another suggested players s**hould have individual / team control over how the game is played out**, consolidating the need/desire to get answers correct before proceeding.

Table 34. Components of the CSD activity students suggested they would amend

Components of the CSD activity students suggested they would amend	*n*
More visuals (pictures and animations)	14
Clear instructions	7
The ability to communicate with other class teams during game play	7
Delete button for all read messages (in order to de-clutter inbox)	7
Work in teams of two, not three – or regularly switch roles to reduce redundancy	5
Work through the game individually	5
Display messages as a conversation rather than email (i.e. like MSN)	4
Webcam - ability to say instead of type responses	3
Ability to choose the characters gender	1
Have individual / team control over how the game is played out (i.e. get answers correct before proceeding)	1
Messages from control room to arrive in students inbox at the same time (simultaneous message delivery)	1

5. Triangulation of results

The key questions to be answered as part of this evaluation are to:

1. Investigate if the game's key cyber-safety messages are identified by students;
2. Measure the short-term impact of CSD on student learning about cyber-safety;
3. Determine if students recognise the link between the cyber-safety messages and how these messages should be assimilated in their own behaviours/lives;
4. Examine the teacher's role in re-enforcing the key cyber-safety messages; and
5. Assess the value of the pre-game and post-game lessons in re-enforcing the key cyber-safety messages.

This section seeks to combine data from multiple sources (stakeholders, teachers, students and game transcripts) to answer the above objectives.

1. Are students able to identify the main cyber-safety messages of the CSD activity?

When asked about the key cyber-safety messages to teach 11- to 12-year-old students, stakeholders responded personal responsibility for cyber-safety was the most important message to instil. In addition, stakeholders reported respectful behaviour and the permanency of students' digital footprint were also key messages to convey.

The main cyber-safety messages promoted in the CSD activity include:

- People who you meet online may not be who they say they are;
- Children should never give out personal information when they are chatting online;
- If children want to meet face-to-face with someone they have chatted, they should always take a parent with them;
- Parents should be involved in and monitor their children's use of the Internet, especially chat rooms; and
- Children should protect their online information and use privacy settings.

These messages match those suggested by stakeholders in that they seek to empower students with actions they can take to be safer online. Moreover, teachers who participated in interviews as part of this evaluation noted these messages are appropriate for the 11- to 12-year-old age group, which this game targets. One teacher suggested:

> *"…technology, be it the net, emails, MSN etc… is part of their life these days. So they have to be made aware of what's going on"* [Scl_004_ST]

In the quantitative survey, students were asked six questions about their behaviour online in regards to engaging with others whom they do not know in person, privacy settings, sharing of information and parent awareness of online friends (Table 19, page 93). Between pre-test and post-test (conducted one to two weeks following CSD activity play) surveys, students' responses to these questions varied little. At both time points, 59% of 11-year-old students reported they only have online friends that they have met in person and 52% said they have set their SNS or IM profile to private. Fewer 11-year-old students reported sharing their password with others at post-test (6%), compared to pre-test (13%); while more 11-year-old students reported at post-test, compared to pre-test, they had blocked or deleted someone who said something they thought was rude or mean (49% to 53%), that they had not shared personal details with anyone (41% to 46%) and they let their parents/caregivers know who is on their friends' list (49% to 54%).

In relation to 12-year-old students, reported behaviour improved from pre-test to post-test in regards to students setting their profile to private (48% to 53%), and not sharing personal details with anyone (44% to 51%). Furthermore, half of those 11- and 12-year-old students who reported using a SNS or IM site also stated they know all their online friends offline and more than a quarter know nearly all their online friends offline (Table 21, page 95).

In general, it appears that some change has occurred in terms of key cyber-safety messages promoted in the CSD activity, with particularly 11-year-olds report of cyber-safety actions increasing between the two time points, albeit a small increase. Nonetheless, while one half of students reported engaging in such cyber-safety behaviours, one half of students also did not report engaging in these behaviours. One reason for this may be the lack of implementation of the pre- and post-game activities which, if taught, may assist in reinforcing the messages promoted in the game. In CSD activity evaluation schools, only

two of 12 teachers reported implementing the pre- and post-game activities; which may have resulted in less reinforcement of the cyber-safety messages promoted in the CSD activity.

2. What short-term impact does the CSD activity have on student learning about cyber-safety?

Focus groups conducted with students immediately following the game give the best understanding of student learning about cyber-safety. Overall, students enjoyed playing the CSD activity (see page 117). While some students commented negatively regarding the time it took to receive responses from guides, they enjoyed the ability to voice their own thoughts and opinions, work in teams and undertake realistic detective work (pages 117 and 119).

When asked about ways the CSD activity made them think about cyber-safety, students reported participation reminded them not to communicate with people online they do not know offline (page 123). Furthermore, students reported the game had increased their awareness of the existence of privacy controls on social networking sites and the need to set these settings to private. As a result of participation, students reported they would limit their SNS profiles to friends and family they know face-to-face, and only accept friends they also know face-to-face (pages 123 and 124).

Some students identified participation in the CSD activity reinforced the concept of 'stranger danger' in an online environment, reporting they now understood how easily others can conceal their true identity online. Participation in the CSD activity also prompted students to be more mindful of the age appropriateness of the social networking site they use and to keep passwords to such sites confidential, even from close friends (page 124).

In addition to reporting actions students would take to protect themselves in the future, after participating in the CSD activity, some students reported they would remove or alter any information they had already placed online in accordance with the messages they had learnt through CSD activity participation. For example, some students reported they would remove or refrain from posting personal information online, both about themselves and about others (page 125).

Participation in the CSD activity also generated a greater understanding among students of the need for parents to be involved in their Internet and computer use. This is evidenced by the suggestion by many students that they would allow their parents to access their SNS profile and/or check the websites they visit. In addition, students reported greater intention to use computers in common areas (i.e., not in their bedroom) and look for secure sites when using the Internet.

When asked what components would be an essential part of a cyber-safety activity, students responded with a variety of considerations to assist in increasing their level of engagement as well as their overall satisfaction with the game. In particular, students highlighted the need for the game to be realistic and interactive, include a reward or points scheme to recognise students for answering correctly, offer a range of scenarios, ensure age appropriate content, enable the exploration of the game environment (e.g., for students to be able to virtually move around the school yard using an avatar type approach), foster teamwork, employ a 'choose your own adventure' type storyline and challenge students (pages 127 to 129).

Further, students offered suggestions for how to improve the existing CSD activity, including:

- the provision of clear instructions at the commencement of the game;
- the ability to communicate with other teams within your own class;
- strategies to enable de-cluttering of the inbox (e.g., a delete button for read messages);
- working in pairs so each student has a defined role and can see the computer screen;
- display messages more like an MSN chat script rather than an inbox as the former is more commonly used by students to interact online;
- the ability for voice responses as opposed to text-based conversations;
- simultaneous message delivery; and
- personalisation options including the ability to choose the genders of characters in the game (pages 130 to 132).

3. Do students recognise the link between the cyber-safety messages and how these messages should be assimilated in their own behaviours/lives?

At both pre- and post-tests, students were asked what they would do if they were contacted online by someone they did not know offline. A list comprising 13 options was provided and students were asked to nominate if they would or would not perform each action. Out of 13 available options, the number of actions students nominated they would do ranged from zero to 13 for 11-year-old students and zero to 12 for 12-year-old students at pre-test, with the average number of actions identified at pre-test being seven for both 11 and 12-year-old students.

Statistical analyses were conducted to determine if the number of actions students reported they would do if contacted online by someone they do not know offline increased between pre- and post-tests. These analyses demonstrated that 11-year-old students, and those students who had a lower than average pre-test score (of the number of actions they selected at pre-test), had a significantly higher action score at post-test (p = 0.004 and < *.001* respectively) (see page 106). This suggests participation in the CSD activity increased their awareness of strategies they could take in this situation.

Moreover, qualitatively, students demonstrated they understood the messages promoted in the CSD activity and intended to alter their online behaviour as a result of participation, as evidenced in the following quotes:

> *"It was a very good storyline – I enjoyed how someone found the phone and you had to try and track who it belonged to. It kind of showed a 'moral of the story' kind of thing – like keeping your profile private and not going [meeting up] with just anyone"* [Scl_007_M]

> *"I think I will be more careful on sites that have anything to do with messaging and if anyone messages me, like strangers I don't know, I think I would just ignore or probably delete them"* [Schl_007_M]

> *"I have my date of birth on my Facebook profile – I will take that down"* [Scl_005_F]

Further, some students showed evidence of critically analysing the game and applying it to real life by stating the game was a contradiction of sorts – advising students not to talk to

people online whom they do not know offline, but in providing this advice (and facilitating the game) students were engaging online with people they did not know in person (see quotes on page 85).

4. What is the teacher's role in re-enforcing the key cyber-safety messages?

During the CSD activity, the main role of a teacher is to supervise students, provide ideas about online safety, help students phrase questions and encourage them to send messages to guides. However, during the evaluation, many schools found it difficult to provide more than one guide to assist in the classroom. This meant that the teacher was simultaneously acting as a guide as well as monitoring classroom behaviour (see pages 65 and 66). In addition, many teachers were unclear of their role as a guide in the CSD activity and found it took time to get used to the CSD activity platform, how to respond to student's messages and what type of response to provide (see page 66). While some teachers enjoyed the challenge being a guide in the game provided, others felt beyond their depth suggesting they would have appreciated more support from those with more experience and expertise in cyber-safety and even for an external guide to visit the school to support the game play (see pages 66 and 67). From the feedback provided by teachers in the evaluation, it appears they felt most comfortable in monitoring student behaviour and prompting student discussion offline, leaving online interaction to those more familiar with the CSD activity platform and with cyber-safety in general.

5. How valuable are the pre-game and post-game lessons in reinforcing the key cyber-safety messages?

While few of the teachers who participated in the game as part of the CSD activity evaluation reported having completed the pre-and post-game activities with students in their class, four of the six long-term evaluation teachers reported they had done so. Some teachers modified the pre-game activity to reduce its duration, or limited pre-game activity to a discussion about Internet use at home (see page 72). The long-term teachers who implemented the pre-game activities felt they provided a good background to the issue for teachers and provided those less familiar with cyber-safety issues and strategies with some guidance on the issue. While those who taught the pre-game activity reported overall positive perceptions about it, several teachers reported from their reading of the pre-game information, they were unclear as to their role in the game play, and would benefit from a succinct overview of the game requirements (see pages 72 and 73).

Those who taught the post-game activity reported this stimulated discussion between teachers and students about cyber-safety provided a good summary of game content and key messages and was a useful guide for class discussion. However, time was a barrier consistently identified by teachers as a reason for not completing the post-game activity (see page 73).

Given the positive comments provided in relation to the pre- and post-game activities by those who implemented them with their class, it seems teachers could be given more direction in the importance of completing these activities around CSD activity participation. Perhaps the succinct summary of teacher roles/tasks mentioned above could specify the completion of pre- and post-game activities as key strategies for maximising students' comprehension of cyber-safety messages. Moreover, due to the time constraints identified by several teachers, it may be useful to detail the key pre- or post-game content, and then list additional points for discussion or supplementary activities that teachers with more time may choose to implement.

Reinforcement of the importance of pre- and post-game activities would also address some stakeholder concerns as to the usefulness of a one-off activity in favour of activities embedded across the curriculum and on an ongoing basis (see page 57). The pre- and post-game activities, and CSD activity play should be offered to teacher and schools as part of a suite of activities promoting cyber-safety messages. The ACMA have a range of resources available to schools which should be promoted actively. For example, in the email sent to teachers as a follow-up to CSD activity participation, the ACMA could suggest other resources the teacher may be interested in.

Both students and teachers reported they would be interested in seeing more scenarios developed to enable students' participation in subsequent years of schooling (see pages 74 and 128). One issue identified by a staff member anecdotally was that students with younger siblings often share the storyline such that the mystery and detective script is ruined for the younger sibling. Offering multiple scenarios would enable schools to implement cyber-safety strategies in consecutive years with less risk of contaminating younger students' knowledge of the storyline.

6. Discussion

The aim of this evaluation was to assess the effectiveness of the Cybersmart Detectives (CSD) activity as an educational resource designed to enhance and improve the cyber-safety practices of young people. A mixed-methods approach was taken with data collected from a variety of sources including students, teachers, national and international stakeholders. This evaluation involved students aged 11-12 years old from Catholic schools in Western Australia who completed quantitative surveys assessing their technology use and cyber-safety attitudes and practices before and after playing the CSD game. A subsample of students also participated in focus groups. Finally, teachers and stakeholders participated in interviews to enable investigation of the functionality of the game and the general use of cyber-safety games as educational resources for students. For clarity, this section will present an overview of the key findings of this study followed by a general discussion.

6.1 Key evaluation findings

6.1.1. Risk group

The most striking results found in this study related to the pre and post-test differences between the risk groups (defined as the number of strategies reported if contacted online by a stranger with fewer strategies indicating high-risk). Most importantly, high-risk students reported significantly more positive actions at post-test than at pre-test. This increase resulted in those students who were classified at pre-test as being high-risk moving into a lower-risk group at the post-test. This result highlights the potential impact of the game on students who are the most vulnerable and at greatest risk for negative and inappropriate interactions online.

6.1.2. Age differences

Some important age differences were found in this evaluation. In contrast to 12-year-olds, 11-year-old students reported significantly more positive actions at post-test than at pre-test. Importantly, 11-year-old students who reported having fewer positive responses if contacted online by a stranger at the pre-test demonstrated a significant increase in the number of skills at the post-test. These results suggest that the CSD game may be particularly helpful for younger students who possess fewer self-protective behaviours.

Interestingly, the largest increase observed between pre and post-test scores for 12-year-olds related to “talking to a teacher” with double the number of students indicating they would do this at the post-test compared to the pre-test (32% at pre-test compared to 68% at post-test). While it is unclear why this increase occurred, it may relate to older students not being aware that teachers are an available resource for support in cases such as was presented in the game (although this same pattern would be expected in 11-year-olds if this was the case). Alternatively, it may be that the older students had an existing negative perception of discussing this type of information with a teacher and the game served to legitimise utilising this resource. In other words, students felt that it was not “cool” to talk to a teacher but seeing this occur in the game highlighted that talking to teachers is a good idea and can facilitate a positive outcome. In this way, the CSD game may also serve to address stereotypes and to encourage positive and self-protective actions.

6.1.3. Risk group profile

Several important differences were noted between the high- and low-risk students in relation to their use of technology and online activities. Overall, the general pattern to emerge from these data highlight the extent to which high-risk students are more likely to interact with strangers online in a variety of contexts (e.g., social networking sites, chatrooms, online games). For clarity, the areas where the difference between the risk groups was largest will be addressed separately.

Internet usage: High-risk students used the Internet on their mobile phone more frequently than low risk students (one to three times per day, High: 15% versus Low: 9%, four to five times per day, High: 5% versus Low: 4% and more than 10 times per day, High: 5% versus Low: 0%). Internet use patterns also differed between the risk groups: high-risk students reported more non-school related Internet use during the week, compared to low-risk students (e.g., about three hours/day – High: 10%; Low: 4%).

Consistently, more low-risk students (41%) used the Internet on an average weekend day for about 1 hour for schoolwork compared to high-risk students (15%), and also for about two hours (15% compared to 7%). Conversely, high-risk students reported using the Internet for a shorter amount of time (i.e., less than one hour) for schoolwork related activities than did the lower-risk students (57% versus 30%).

Location of Internet usage: When at home, 48% of high-risk and 59% of low-risk students reported they usually use the Internet in an open area and 50% and 44% (respectively) reported using the Internet in the study or separate room. Interestingly, similar percentages (22%) of students reported using the Internet in their bedroom suggesting that only considering the location of a computer may not reveal the extent to which young users are at risk. In other words, students who use computers in open spaces may still be at high-risk for inappropriate contact from strangers as a result of their online activities and behaviours. This result indicates the importance of proper parental supervision over and above the location of a computer.

Online activities: More high-risk (73%) compared to low-risk (59%) reported having a social networking site or instant messenger profile and using it for longer (14% of high-risk students used it up to two hours a day compared with 8% of low-risk students). Importantly, more high-risk students reported using online chat sites (66% versus 44%). While similar percentages of students in both risk groups reported playing games on the Internet (High: 81%; Low: 72%), more low-risk students (35%) reported they play online games that don't involve other people compared to high-risk students (14%). Importantly, more high-risk (49%) compared to low-risk (16%) students reported playing online games with both people they know and those they have never met.

Online interactions: Interestingly, few differences were found between the risk groups in relation to their use of social networking sites. Despite the lack of differences, some concerning trends were noted in all students who participated in this study. For example, more than half of students in both risk groups reported having friends online that they have met offline (High: 57%, Low: 51%) with only 57% of high-risk and 44% of low-risk students knowing all or nearly all of their online contacts offline. In addition, most students have not set their SNS profile to private (High: 61%; Low: 57%) and more than a third of students shared their password with someone (High: 34%, Low: 43%). Interestingly, more high-risk students reported that they had let their parents know who was on their SNS friend list. Thus, contrary to expectations, it appeared that lower-risk students engaged in fewer protective strategies than did the higher-risk students. As this issue was not explored in this project, it is not possible to understand why the lower-risk students engaged in fewer protective behaviours. However, it may be that they felt more confident given that they had more strategies to address inappropriate contact if it occurred.

These results reveal interesting safety practices amongst 11 and 12-year-olds especially in relation to the people they have contact with over the Internet. It is concerning that the majority of students are interacting with individuals they do not know offline. Of course, based on the data collected, it is not possible to know if the people whom students are in contact with are of a similar age or older or are known to the friends they do know offline (i.e., friends of friends). Furthermore, it is not possible to know the nature and extent of the online interactions that students are having with these individuals. For example, if they are online friends on a SNS they may only have indirect interactions (i.e., no direct contact but can view online posts, pictures and discussions). Even if these interactions are indirect, there is a clear risk to sharing personal information with people that are not known offline and this issue should be a clear priority for cyber-safety messages.

6.1.4. CSD enjoyment factors

An important factor in the success of any game is the extent to which it is enjoyable for the intended audience, although this is more important in games which have been developed for entertainment purposes only (Bostan & Ogut, 2009). All participants (including teachers) were asked if they enjoyed playing the CSD game and the majority responded in the affirmative. The key factors that students enjoyed more were explored with the majority indicating they liked the interactive nature of the game (i.e., answering questions and receiving feedback). Overall, the feedback from students and teachers was positive. The basic concept of using a computer game approach was appealing to young people as it was fun, engaging and contextualised their learning experience. This is consistent with other areas of psychological research highlighting the importance of ensuring that young people are cognitively and emotionally engaged in the activity and the benefits of using ICT to facilitate this (Dooley et al., under review).

As was supported by the comments of both students and stakeholders, presenting safety information in the appropriate context is an important element of an effective approach to cyber-safety. Indeed, the majority of the teachers interviewed indicated that cyber-safety messages targeted to students using the CSD game were very appropriate or appropriate given the role of technology in their everyday life. In addition, the supportive role that the CSD game (and similar cyber-safety resources) could play is important to highlight.

The real-time interaction capability of the CSD game was highlighted by most students as an element that was very appealing about the game. This is an important issue

as it indicates that synchronous communication formats may be a key factor in communicating cyber-safety messages. In the fast-paced social world of the average young person, asynchronous interactions may not serve to hold their interest in an activity and the more the real-time look and feel a task or game can be, the more engaging it is likely to be. In this sense, text-based messages are unlikely to be easily transferable to an ICT-based interaction especially for younger students. In addition, real-time interactions are more likely to closely mimic daily interactions and this, in turn, can have important implications for the extent to which messages become part of a students' response repertoire. The more response options that a student has when faced with a difficult or inappropriate social interaction, the more likely positive, non-aggressive behaviours will be used (e.g., Crick & Dodge, 1994, 1996; Dooley, Shaw & Cross, in press; Orobio de Castro, Veerman, Koops, Bosch & Monshouwer, 2002). Ultimately, this results in a more favourable outcome and resolution of a social problem.

Furthermore, the CSD game provides students with a valuable opportunity to practice cognitively and emotionally processing, evaluating and responding to a highly inappropriate social interaction. This safe exposure to dangerous situations is, for obvious reasons, not easy to achieve. Despite young people being provided with relevant safety messages (i.e., stranger danger) from a young age, it is likely to be somewhat rare that they have an opportunity to practice personal safety in an ICT environment in a situation of immediate danger. Having opportunities to practice social problem solving skills in an environment that matches the environment within which these skills are likely to be used is a significant strength of the CSD game.

This type of context and domain-specific learning is exceptionally important especially for younger students whose social problem solving and coping skills are still emerging and are typically less effective and more inappropriate than older students (Mayeaux & Cillissen, 2003; Takahashi, Koseki & Shimada, 2009). Although no specific age has been identified as the time when social problem solving and related skills develop, there is some evidence of a developmental shift in sociocognitive functions (cognitive processing in social situations) between 6 and 8 years of age (e.g., Livesly & Bromley, 1973; Yeates & Selman, 1989). Interestingly, recent evidence of the use of ICT demonstrated that a fundamental change in how young people use technology occurs from eight years of age (Gutnick, Robb, Takeuchi & Kotler, 2010).

Given the number of 11 and 12-year-old students who reported having a social networking site in this project, it would seem reasonable to assume that many users are even younger. In fact, evidence from the USA suggests that as many as five million Facebook users are younger than ten years of age (Kang, 2011). Thus, these young people are clearly unlikely to have fully developed social problem solving skills. In fact, they are not yet fully neurologically developed with the frontal lobes (the part of the brain responsible for disinhibition, planning, organising and social problem solving) still not yet fully formed. Given this fast-paced ICT environment, real-time synchronous communication, challenging social problems and a developing body and mind, the potential for a young person to generate inappropriate and ineffective solutions is high. Such is the impact of fast-paced and real-time communication that strong evidence from other areas of psychological and neuropsychological research highlights the impact that a short delay has between a stimulus and the inappropriateness and aggressiveness of a response with young people generating less aggressive responses when there is about a 10 second delay (e.g., Dooley et al., 2008).

Given the development of mobile communications and Internet-ready mobile phones (where online interactions can occur at any time and in the midst of many distractions, e.g., while using a social networking site in a school yard where there is lots of noise), the need to develop cyber-safety skills that students can use in real-time interactions is of critical importance. As more young people use the Internet on their mobile phone (and use desktop computers less), the need to be able to quickly identify, assess, evaluate and solve potential problems involving strangers online becomes more important.

Another important issue to emerge was in relation to the supportive transferability of the cyber-safety messages in the game. Many teachers felt that a significant advantage of the CSD game was that it enabled them to reinforce the cyber-safety messages that they were already teaching in their classrooms. Although the core story of the game is fixed (i.e., the characters, the problem, the clues presented to students), the capacity for guides to provide unstructured feedback is an important aspect of the potential flexibility of the game. For example, guides can use the game to comment on current events as the nature of their feedback is not restricted by the game. This can be an important element in supporting the cyber-safety work that teachers, schools, parents, research, educators and government agencies engage in.

It is important to note that some limitations were raised by participants in this evaluation. As is common in non-curricular school activities, many teachers commented on the perceived amount of time needed to organise the CSD game (up to 2 hours in some cases). A consistent concern raised by teachers (in many of the school-based research projects conducted by the CHPRC) was that time is a very valuable commodity and the demands of teaching and related activities do not always permit engaging in additional activities. It is clear that some amount of time is necessary to properly orient users (teachers and students) to the game, its objectives and the manner in which it operates.

It is important to note that, while every effort was made to ensure that the administration of the game was as similar to a non-evaluation project administration (i.e., would be done by the ACMA as part of a standard administration), participating in the research project added some additional tasks for teachers above and beyond actually playing the game. In addition, teachers were asked to comment on the game content only and their impressions of the time involved in organising and playing it. Consistently, most teachers reported that they did not read the instruction manuals and nearly all teachers did not complete the debriefing session with students once the game was finished. This latter information was supported by informal feedback from the ACMA. This was unfortunate as the debriefing session holds a significant potential to raise and address some important issues in relation to cyber-safety and online activities in students.

In addition, staff shortages meant that many of the teachers who participated in this evaluation were the only guides provided by the school (with no opportunity to recruit additional guides). As a result, many suggested that acting as guide and managing student classroom behaviour during the administration of the game was challenging. The ACMA has provisions and procedures in place to aid schools to locate and obtain assistance with guides and, in all cases, provides this support directly. The lack of awareness of this by teachers in this evaluation may be a function of their lack of familiarity with the game process (i.e., not properly reviewing the materials). Of course, this is likely to relate to the amount of time that teachers have to dedicate to the game and its set-up.

The long-term applications of the game were raised in the qualitative interviews and focus groups with teachers and students. Specifically, the game is intended as a cyber-safety resource to be used on only one occasion. The very nature of the unfolding mystery of the story means that students will not have the same reaction if they were to sit and play

the game for a second time. Of course, the integration of the CSD game into other cyber-safety resources will likely result in a consistent, comprehensive and broader approach to increasing the knowledge and awareness of safety issues. In addition, the stand-alone nature of the game means that administration is not dependent on other resources.

That several teachers and students suggested that the game be developed further to enable users to choose from a range of scenarios based on individual and individual school needs highlights the extent to which they felt that variety in the issues presented is important. However, there are many challenges when examining the extent to which the game impacts on an individual user's personal safety practices and behaviour when the incidence of sexually predatory behaviour is relatively low (see Dooley et al., 2009 for a comprehensive review of the evidence of cyber-safety risks). So, the call for variety in scenarios might reflect the extent to which students (and teachers) did not personally connect with the situation. In other words, the situation in the game might not prompt them to change their behaviours because they don't believe they would ever be in that situation in the first place (or don't know anyone who has been). Of course, it is also possible (and more likely in the context of the other positive feedback obtained) that the call to include more scenarios stems from recognising that the game has value and many potential benefits as a resource to enhance cyber-safety. Thus, if it works in one context, it is likely to work in others.

It should be noted that the greatest strength of the CSD game may be in the approach taken to present the scenario (i.e., gradually presenting clues and providing participants with an opportunity to chat and ask questions not directly related to the game itself). In terms of inappropriate contact, the greatest risk to young users of technology is in the form of cyber-bullying (Dooley et al., 2009). Although cyber-bullying rates are likely to be significantly higher than the type of online deception and attempted abduction described in the CSD game[13], the reported prevalence rates of cyber-bullying in Australia are still lower than offline bullying (Cross et al., 2009). The broad nature of the CSD game facilitates discussions of the risk factors for exposure to those types of negative interactions that go beyond sexual predation and abduction and can cover other types of risky interactions (e.g.,

[13] "Likely" is used as there is currently no prevalence data available on the incidence of deceptive online contact resulting in attempted offline abduction in Australia.

cyber-bullying). Thus, the game can permit guides to comment on issues around privacy, personal information management and digital reputation.

6.2 CSD and student cyber-safety

The primary question of interest in this evaluation was the extent to which the game impacted on student knowledge, awareness and reported cyber-safety strategies. To assess how the game performed in relation to student cyber-safety strategies, a pre-post game design was used. As presented in the literature review, very few cyber-safety programs have been subjected to a methodologically rigorous evaluation making it somewhat difficult to specifically identify the key components that should comprise an effective cyber-safety game. In addition, there are many challenges to identifying and measuring changes in actual behaviours as opposed to intended behaviours.

One of the challenges with providing support services to students who experience negative situations is being able to identify who those students are. Thus, providing students with the skills to know where, when and how to seek help is an important aspect of being and staying safe online. Dooley and colleagues (Dooley, Gradinger, Strohmeier, Cross & Spiel, 2010) reported that Australian and Austrian students who were victimised online were significantly less likely to report these experiences than were students who were victimised offline. In addition, males were significantly less likely to report when compared to females. Thus, increasing student confidence and competence to seek help when necessary is one of the most important elements of any cyber-safety resource. As such, the extent to which the CSD game was associated with self-reported actions (if victimised) was an important question for this evaluation.

While many pre/post-game administration differences were noted, few were statistically significant (these are discussed in the CSD and risk status section). Despite the lack of statistical significance, several positive results were found. Overall, a greater effect was noted for younger students (11 year olds) than older (12 year olds) with more of the former reporting significantly more actions at the post-test than the pre-test. Although the mechanism behind this is unclear (given it was not explored in the student qualitative interviews), it may be that the game was more of a novelty to younger students and, as a result, they attended more to the activity and retained more information. Alternatively, older students may have been exposed (through personal practices, friends, media or through

other avenues) to risky situations online and did not believe that some of the actions were effective methods of addressing inappropriate contact. While no data was collected as part of this project, there is evidence from other areas of cyber-safety indicating that older students are more likely to be victimised or subjected to inappropriate contact online from strangers than are younger students (see Dooley, et al., 2009 for a review). Support for the argument that the age difference was based on being more engaged in the game is found in relation to the recall of game information. Overall, younger students performed better at recalling the details of the game (e.g., age of main character, Sarah, in game, Sarah's mobile phone number obtained online, age of the person waiting to meet Sarah).

In addition, gender emerged as an important factor in relation to the extent of and types of actions that students reported they would engage in if victimised. Overall, girls reported that they would engage in all actions to a greater extent than did boys (with the exception of talking to a teacher/principal or the police). In addition, several differences were found between boys and girls pre/post endorsement of actions. For example, the number of boys who reported they would contact the police or talk to a friend increased between the two assessments. However, while more girls at post-test than reported talking to the police, fewer indicated they would talk to a friend.

In general, only minor differences in the actions taken on SNS or IM sites were noted between pre and post-test assessments for both boys and girls. However, some important trends were found. For example, for both genders, the percentage of students who reported sharing passwords with others decreased from the pre to post-test. This may be because the students realised as a result of playing the game that sharing passwords is not a safe practice. In addition, a small reduction (5% for boys, 3% for girls) in the numbers of students who reported that their SNS profile was not set to private was found. Given that over one-third of students reported not using SNS, the small sample sizes in each category did not permit the examination of statistical difference between the two assessment points.

6.3 CSD and risk status

Possibly the most important potential for the CSD game (and all cyber-safety resources) is the potential to impact on the safety practices of the most vulnerable users. This issue has not specifically been addressed in previous evaluations but the importance of considering the challenges of users who are most at risk has been noted by some (e.g., Wishart et al., 2007). Given the complexity with defining and operationalising "vulnerability" we opted for an alternate approach. We aimed to identify a sub-sample of students who might be more at risk for negative outcomes associated with inappropriate contact online. On the basis of other research evidence suggesting the link between actions and poor mental health after cyber-victimisation (e.g., Dooley et al., under review), we contrasted students who reported the lowest number of actions in response to online contact by a stranger with students who reported the highest.

When comparing these two groups (which we described as high-risk and low-risk), it was found that exposure to the CSD game was associated with a significant increase in the variety of actions that young people report they could take if approached online by a stranger. This result was most pronounced for students who, at the pre-test assessment phase, reported the lowest levels of action strategies and, as a result, were classified as being at high-risk. Students in this high-risk group not only reported significantly more strategies at the post-test assessment, but also moved out of the high-risk category (their average action score was within one standard deviation below the mean for the overall group). Consequently, it is likely that the CSD game may be most effective with the most vulnerable user group.

This result represents a major finding in relation to cyber-safety resources and is a significant addition to the scientific evidence supporting the use of the CSD resources with students. Of course, the limitation associated with this (and all other) findings is that it is only intended behaviours that are measured and not actual behaviours. Nonetheless, the significant increase in the reported actions by the most at-risk students in this sample illustrates that these cyber-safety educational resources can be used as a means to enhance awareness and knowledge of the types of actions that can be undertaken if confronted by an inappropriate situation online.

Finally, a comment on the sample involved in this study is warranted. Although the students who participated were students from Catholic schools in Western Australia, their reported ICT use patterns was mostly consistent with previous data released by the ACMA. For example, just less than 100% of all the students in this study reported using the Internet for less than 3 hours on an average weekday. Consistently, students aged between 10-13 years reporting using the Internet between 1.5-2.3 hours per day (ACMA, 2009). Thus, while it is not possible to directly compare students in this study with all other students in Australia, on the most basic issue of Internet usage, this sample was consistent with other national data.

6.4 Conclusion

This evaluation aimed to examine the effectiveness of the Cybersmart Detectives activity – a cyber-safety resource aimed at 11-12 year olds. A large variety of data were collected from national and international stakeholders, teachers, students and staff from the Australian Communications and Media Authority. Overall, the effectiveness of the game as a beneficial cyber-safety resource was established. Using a pre-post design, it was demonstrated that the most vulnerable students (those who were considered at high-risk as a result of having fewer response strategies if contacted by a stranger online) significantly increased the number of strategies they could employ. Given the dearth of research in the area of cyber-safety resource evaluation, it is difficult to interpret the findings of this study in relation to other research literature. For example, several of the program evaluations described in the introduction reported mixed and statistically non-significant results (e.g., Missing Program).

In part, this is due to the difficulty in measuring behavioural change in relation to relatively rare experiences. As such, most evaluations measured intended behaviour (i.e., what a student *would* do if they were contacted), which is not an accurate measure of *actual* behaviour. For this reason, this evaluation was focused on examining the extent to which exposure to the game resulted in an increase in the skills of younger users. In conclusion, the results of this program evaluation provide good evidence supporting the CSD game as an important and valuable cyber-safety resource. The evidence presented suggests that the game is most effective with vulnerable youth and those who demonstrate fewer safety practices.

7. Appendices

Appendix 1. Supplementary results

This section comprises analyses additional to that outlined in the evaluation brief initially submitted to the ACMA, but discussed over the course of the evaluation period. In this section, results are presented in relation to team results (questions posed, answered, flagged and deleted), responses to poll questions collected during game-play and thematic analysis of the nature of the questions posed and answered during game-play.

Demographic characteristics of schools

During the evaluation period, students at 75 schools (including those involved in the evaluation) played the CSD activity (Table 35). These schools represented all Australian states: Western Australia (33%), New South Wales (25%), Victoria (20%), South Australia (10%), Queensland (5%), Tasmania (3%), the ACT (1%) and the Northern Territory (1%). Half of the schools were public schools (55%), while one-third (31%) were from the Catholic sector and 15% were Independent schools. Across these 75 schools, 264 guides facilitated students' learning comprised of 37% ACMA staff, 56% volunteers (e.g., school staff) and 19% police.

Table 35. Demographic characteristics of schools who played CSD in evaluation period

		%	*n*
State	ACT	1	1
	NSW	25	19
	NT	1	1
	QLD	5	4
	SA	10	8
	TAS	3	2
	VIC	20	15
	WA	33	25
Sector	Catholic	31	23
	Independent	15	11
	Public	55	41
Guides	ACMA staff	37	97
	Police	7	19
	Volunteers	56	148

A1.1 Team results

At the end of the data collection period, the ACMA provided the CHPRC research team with several Microsoft Excel spreadsheets containing statistics relating to the number of questions each team asked online during the CSD activity, the percentage of questions answered by guides, the percentage of questions flagged and the percentage of questions deleted during administration of the CSD activity.

In the 23 CSD activity administrations comprising the dataset, a total of 7,911 questions were posed by the 439 teams that played the CSD activity. The average number of questions posed by an individual team was 18, and the range was 0 to 53. On average, 79% of a team's questions were answered by the CSD guides. The percentage of a team's questions that were answered ranged from zero to 100%. Less than 1% of a team's responses were flagged (0.2%), with this figure ranging from 0% to 17% of a team's questions. Student comments were flagged if they disclosed information that may be of concern (e.g., that they had been cyber-bullied). Finally, a small number of each team's

questions were deleted from the game screen (9%), which equates to, on average, two questions per team.

A1.2 Poll question team responses

Throughout the CSD activity, students are provided with 15 multiple choice questions to facilitate the learning process (Table 36).

Table 36. Poll questions in CSD activity

	Poll questions
1	What would you do if you found someone else's mobile phone?
2	Do you think that students should be able to use a mobile phone at school?
3	Which of the following details should you never post on profiles on the Internet?
4	Why do you think schools have rules about Internet use?
5	If you had a problem and thought that you couldn't talk to a teacher or parent about it, who would you talk to?
6	Before today, did you know that Internet profile pages usually have privacy settings that let you control who gets to see your page?
7	What would you do if you thought someone was in trouble?
8	What would you do if you thought a friend was being bullied or upset about something?
9	Did you know that putting photos on the Internet that show what you look like with personal details like where you live, go to school, your team, your address or phone number could put you in danger?
10	Which of the following do you think people on the Internet could lie about?
11	Why do you think teachers and parents talk to each other?
12	Where do you think is the best place to have a home computer?
13	What number do you use to call the police in an emergency?
14	Can you believe everything that people tell you on the Internet?
15	If someone you met in a chat room asked to meet you in person, would you: say yes but make sure you took your parents or an adult with you; say yes and go on your own to the meeting; or say no to the meeting?

When each poll question was posted in the game activity, several response choices were also provided. This section presents first, the demographic characteristics of the teams who played the CSD activity in the evaluation period (9 June to 19 October), and second, the results of each team's answer selection.

1. What would you do if you found someone else's mobile phone?

Of the 946 known teams who played the CSD activity during the evaluation period, 913 (97%) responded to poll question one (Table 37). The majority of teams said if they found someone else's mobile phone they would hand it in to a teacher or someone in charge (73%).

Table 37. Team responses to action if find someone else's phone

	%	*n*
Keep it and use it	2	19
Hand it in to a teacher or someone in charge	75	667
Put it back where you found it	3	32
Try to find who's phone it is	21	195

2. Do you think that students should be able to use a mobile phone at school?

All known teams (100%) answered poll question two (Table 38). When asked if students should be able to use a mobile phone at school, the majority of teams thought this was important for emergency calls only (74%).

Table 38. Team responses to students' mobile phone use at school

	%	*n*
Yes	15	140
No	11	102
For emergency calls	74	704

3. Which of the following details should you never post on profiles on the Internet?

Of the 96% of teams who answered poll question three, the majority (84%) responded details about all items listed (full name, age or date of birth, any phone numbers, home address, your school and bank account details) should not be posted on profiles on the Internet (Table 39).

Table 39. Team responses to availability of details on the Internet

	%	*n*
Full name	1	13
Age or date of birth	1	4
Any phone numbers	1	4
Home address	6	57
Your school	1	5
Bank account details	7	61
All of the above	84	767

4. Why do you think schools have rules about Internet use?

Of the 946 known teams who played the CSD activity during the evaluation period, 94% answered poll question four (Table 40). The majority of teams reported that schools have rules about Internet use to help keep students safe (64%).

Table 40. Team responses to purpose of school rules about Internet use

	%	*n*
To keep costs down	1	4
To keep the network fast	0	0
To help keep students safe	64	570
To make sure the school network is safe from viruses	3	30
All of the above	29	257
To stop you having fun	3	30

5. If you had a problem and thought that you couldn't talk to a teacher or parent about it, who would you talk to?

Of the 97% teams who responded to this poll question, the majority (93%) of students reported they would seek additional support from someone they have met and could trust if they were not able to talk to a teacher or parent about a problem they were facing (Table 41).

Table 41. Team responses to sources of support when facing a problem

	%	*n*
Friends I've met online	1	4
Someone I've met and could trust	93	847
No one	7	63

6. Before today, did you know that Internet profile pages usually have privacy settings that let you control who gets to see your page?

Of the 946 known teams who played the CSD activity in the evaluation period, 95% completed poll question six (Table 42). Most students were either aware of the existence of privacy settings (43%) or were aware and had set their profile page to private (49%).

Table 42. Team awareness of privacy settings on Internet profile pages

	%	*n*
Yes	43	385
No	9	77
Yes, I have set my profile to private	49	439

7. What would you do if you thought someone was in trouble?

Poll question seven was completed by 93% of teams who played the CSD activity during the evaluation period (Table 43). The majority (84%) of teams reported they would tell a teacher if they thought someone was in trouble.

Table 43. Team responses to actions if someone was in trouble

	%	*n*
Tell a teacher	84	743
Look for them yourself	9	77
Mind your own business	7	61

8. *What would you do if you thought a friend was being bullied or upset about something?*

Of the teams who played the CSD activity during the evaluation period, 92% answered poll question eight (Table 44). When asked what they would do if they thought a friend was being bullied or upset about something, just over half of students reported they would do a number of actions to assist them including telling a teacher, telling a trusted friend and trying to convince the friend to seek help (55%). A further one-fifth (21%) of students reported they would try to convince their friend to seek help if they thought they were being bullied or were upset about something.

Table 44. Team responses to actions if a friend was upset or being bullied

	%	*n*
Tell a teacher	19	163
Tell a friend you trust	3	26
Try to convince them to get help	21	182
All of the above	55	482
Do nothing	2	20

9. *Did you know that putting photos on the Internet that show what you look like with personal details like where you live, go to school, your team, your address or phone number could put you in danger?*

Of the teams who responded to this poll question (93%), the majority (93%) reported they were aware that putting photos on the Internet that show what you look like with personal details like where you live, go to school, your team, your address or phone number could put you in danger (Table 45).

Table 45. Team responses to awareness of dangers of uploading personal details/photos

	%	*n*
Yes	93	813
No	2	18
I don't need to worry about that because I can look after myself	5	45

10. Which of the following do you think people on the Internet could lie about?

Of those teams who responded to this poll question (90%), the majority were aware that people on the Internet can lie about many personal details including their name, age, photo and where they are (93%; Table 46)

Table 46. Team awareness of ability for information on Internet to be untruthful

	%	*n*
Their name	1	7
Their age	3	30
Their photo	1	7
Where they are	1	4
All of these	93	793
None of these	2	15

11. Why do you think teachers and parents talk to each other?

Most teams (94%) responded to poll question 11 (Table 47). The majority (93%) of teams reported teachers and parents talk to each other about a variety of issues including school work, problems and bullying.

Table 47. Team responses to topics discussed by teachers and parents

	%	*n*
School work	1	9
Problems	3	23
Bullying	2	14
Any of the above	93	827
None of the above	2	14

12. Where do you think is the best place to have a home computer?

Of the 946 known teams who participated in the CSD activity during the evaluation period, 92% responded to poll question 12 (Table 48). The majority (90%) of teams reported the best place to locate the home computer was in a public room like the living room.

Table 48. Team responses to best place to locate the home computer

	%	*n*
In your bedroom	10	88
In a public room like the living room	90	779

13. What number do you use to call the police in an emergency?

The majority of teams who responded to poll question 13 (89%) reported the number to use to call the police in an emergency was '000' (65%) (Table 49). A further one-third (31%) of teams were aware that in addition to '000', '112' can be dialled to access the police in an emergency using a mobile phone.

Table 49. Team responses to phone number used to call police in an emergency

	%	*n*
000 from anywhere	65	550
112 for mobiles	2	15
911	2	13
Both A & B (000 from anywhere and 112 for mobiles)	31	263

14. Can you believe everything that people tell you on the Internet?

Of the 946 teams who played the CSD activity during the evaluation period, 89% responded to poll question 14 (Table 50). Almost all (99%) students were aware that you cannot believe everything that people tell you on the Internet.

Table 50. Team awareness of the truthfulness of information provided on the Internet

	%	*n*
Yes	1	11
No	99	833

15. If someone you met in a chat room asked to meet you in person, would you: say yes but make sure you took your parents or an adult with you; say yes and go on your own to the meeting; or say no to the meeting*?*

Of the 946 teams who played the CSD activity during the evaluation period, 84% answered poll question 15 (Table 51). The majority (74%) of students reported they would say 'no' if someone they met in a chat room asked to meet them in person.

Table 51. Team responses to meeting someone they met in a chat room

	%	*n*
Say yes but make sure you took your parents or an adult with you	25	200
Say yes and go on your own to the meeting	1	3
Say no to the meeting	74	587

A1.3 Game transcription

A total of 49 CSD activity transcripts (i.e., communication between teams and guides) were recorded and provided to the CHPRC research team by the ACMA for analysis. After coding 28 transcripts, the identification of themes had reached saturation point and coding was terminated. The demographic characteristics presented in Table 52 display the number of schools in each state and sector for all transcripts. In total, 75 schools are included in the transcripts provided by the ACMA covering CSD activity administration from June to October. The majority of schools represented the Government / Public school sector (56%, *n* = 42), followed by Catholic (29%, *n* = 22) and Independent schools (15%, *n* = 11). One-third of schools (33%, *n* = 25) represented Western Australia, of which, nine were involved in the CSD evaluation. One-quarter of schools were located in New South Wales (25%, *n* = 19), followed by Victoria accounting for 20% of schools (*n* = 15), South Australia (11%, *n* = 8), Queensland (5%, *n* = 4) and Tasmania (3%, *n* = 2). The ACT and the Northern Territory were each represented by one school (1%).

Table 52. Characteristics of schools comprising game transcripts

		%	*n*
State	ACT	1	1
	NSW	25	19
	NT	1	1
	QLD	5	4
	SA	11	8
	TAS	3	2
	VIC	20	15
	WA	33	25
Sector	Catholic	29	22
	Government / Public	56	42
	Independent	15	11

In the 49 game transcripts, 265 guides helped facilitate student's game play (Table 53). The majority of these were volunteers such as classroom teachers and IT specialists in schools (56%, *n* = 148), followed by ACMA staff (37%, *n* = 99) and Police (7%, *n* = 18). The number of guides facilitating each game play ranged from two to 26, with on average six

guides per CSD activity. The number of each type of guide involved in each state was explored to determine any differences in facilitation of the game. While the number of ACMA staff and volunteer guides was highest in WA and NSW, these were also the states with the highest number of CSD activities played during the evaluation period.

Table 53. Guides involved in CSD activities

		%	n
Guide	ACMA staff	37	99
	Police	7	18
	Volunteer	56	148
ACMA staff	ACT	2	1
	NSW	26	15
	NT	2	1
	QLD	3	2
	SA	10	6
	TAS	3	2
	VIC	19	11
	WA	34	20
Police	ACT	5	1
	NSW	10	2
	NT	5	1
	QLD	5	1
	SA	10	2
	TAS	5	1
	VIC	25	5
	WA	35	7
Volunteer	ACT	2	1
	NSW	28	15
	NT	2	1
	QLD	4	2
	SA	11	6
	TAS	4	2
	VIC	18	10
	WA	31	17

The following discussion presents main student and guide findings resulting from thematic analysis of these CSD activity transcripts.

Student comments, responses and questions

The large majority of student communication made during the CSD activity play was in **response to guide questions or scenario questions**. For example:

"Mr. Saunders wants her to be safe. Ask a teacher. And if it gets really out of hand ask the police"

"We think you should maybe ask the teachers a few grades lower than Georgia who Sarah is and show them the phone"

"Yes we do think it is a case of bulling"

"I'd probably be worrying, because I'd be wondering if Sarah had actually ever met Kel before. I'd keep looking for Sarah"

This indicates students are highly engaged in the CSD activity when guides provide questions that prompt students to think critically. Further, guide questions such as those presented above enable students to actively assess their level of cyber-safety awareness, highlighting ways by which this may be improved or amended. Therefore, the types of guide responses and questions provided to students play an integral role in the level of student engagement with the CSD activity.

Students also spent a portion of game play making **general conversation** with their guide/s, comments such as: *"Who R U?", "Hey, guides, I am really excited to meet you! We could become really good friends! Best Buddies, something like that! Well, got to go!"* and *"Hello, what are you up to guides"* are a common part of general conversation. Such conversation indicates students were excited about the game play and curious about the identity of their guide/s.

Students commonly thanked the guides for their help throughout the game, which demonstrates that they enjoyed participating in the game. The quotes below reflect this:

"Laterz bru'z yeeeeeew"

"Ok cya thanks for letting us do this activity bye"

"Thank you for the fun!!!!!!!!"

"Thanks for this lesson"

As the CSD activity progressed, students began to ask **questions regarding game content or scenario**, such as "*is the person eating lunch getting bullied?*"

"Does Kel go to the same school as Sarah?"

"Is Sarah at her class?"

This suggests students comprehend the game content and connect with the scenario as they were seeking further details to elaborate or clarify the story. Importantly, this interaction suggests students embraced their role as a detective in the CSD activity.

Similarly, each scenario question required teams to think laterally to investigate and arrive at an appropriate solution. Therefore, many questions were asked about the **game process**, specifically 'what to do':

"Hey is it possible to go wif Georgia to go find Sarah?"

"Should we try and look for her or get more info or somtin like dat???"

"So how do we find where she is and stop him doing anything serious???"

"Do u have to answer the purple messages?"

A very small portion also posed **questions regarding game functions** (i.e., how to send a message). This indicates some students required prompts in order to understand how to investigate each scenario and proceed through the game.

A small portion of student communication was made in **response to guide feedback**, specifically, making positive comments including *"why thank you", "thanks for letting us know", "yeah, that's a great idea to ask a teacher"* and *"great advice :D is there any other ways to keep safe on the Internet?"*. This indicated some students value the reassurance provided by encouraging guide commentary.

A very small portion of student communication during CSD activity play was to make a **positive question or response regarding game content or scenario** (i.e., this is fun).

An even smaller portion of students communicated a **negative question or response regarding game content or scenario** (i.e., this is boring).

Guide comments, responses and questions

Three types of guides are recruited to help facilitate the CSD activity play; ACMA staff, police and volunteers (e.g., classroom teachers, IT specialists and parents). This section describes the comments, responses and questions guides posed to students during game play in the 28 transcripts reviewed. As the differing experience of guides may influence the nature of the comments they post in the game play, discussion of themes is presented separately for each type of guide.

The ACMA staff guides

The ACMA staff posted 2,097 of the 4,080 comments posted by guides during CSD activity sessions between June and October, 2010. The ACMA staff guides posted many comments that provided **reassurance and encouragement** to students that they had posed an appropriate response to scenario questions or had understood the process of game play:

"Wow, team 5! You really know how to be cyber safe! Keep up the good work!"

"Excellent response team 1."

Some of the ACMA staff guides also posed comments that **provided guidance** to help students answer scenario questions and critically evaluate the scenario. Often this was as simple as *"what do you think?"*, but rather than answering the question for students, they reflected the question to generate discussion amongst teams playing the CSD activity:

"I'm not sure that you'd be able to find the name Rolergirl in the white pages. How else can you search for that name?"

"The police can definitely help. Who can help at your school?"

Further, a few of the ACMA staff guides provided responses to enable students to **think critically** about the game scenario and apply this to their own situation or 'real life' outside of the CSD activity:

"Do you set your profile to private?"

"Why do you think that schools have rules about using the Internet?"

"OK, but what would you do with the phone?"

A small portion of comments posted by guides involved **general conversation** with students. Often, this occurred at the beginning of the CSD activity, when building a rapport with students and getting them interested in the activity, as well as at the end of the CSD activity, when thanking students for their participation.

A few of the comments posted by the ACMA staff guides **answered questions regarding game content** posed by students to assist with their comprehension of the CSD scenario:

"We are not exactly sure yet. Georgia has said that Sarah told her he was 17"

On occasion the ACMA staff guides **provided cyber-safety advice** to students during game play, usually that related to the scenario unfolding in the CSD activity:

"It is important that parents and their children know how to use the Internet safely. Parents can also learn about online safety by researching online or taking a class."

"It is always a good idea to talk to someone if you feel uncomfortable or confused about a situation. The sooner the better! A friend can help and a parent or teacher will definitely have some good ideas for coming up with a solution."

"You can't trust people that you do not know online, because you do not know if they are being truthful. This is why you should keep personal information private by not sharing it online."

A small number of the ACMA staff guide responses assisted students in navigating the game portal, in particular to **answer students' questions about the game process** (i.e., how to find something):

"What don't you get team 10? The story line will be sent out in the purple messages. You need to read them (from the bottom of the screen first as they are the oldest ones) and answer the questions in the clues to try to help Sarah. OK?"

"Read the purple messages and answer the questions by sending a response to the guides. Ok?"

A very small number of the ACMA staff guide responses included comments providing their own **personal opinion**.

Police guides

Police guides posted 64 comments (of the 4,080 comments posted in total) across the 28 transcripts reviewed to identify themes in response content. Many police guides' comments related to prompts to assist students to **think critically** and relate the CSD scenario to their own life:

> *"Why do you think it is good to talk to your parents about what you do on the Internet and computer?"*

Some police guides posted comments to provide **reassurance and encouragement** to students or to **provide guidance** to assist with moving students through the scenario:

> *"I totally agree. She should have spoken only to people she knew."*

A small number of police guides **responded to students' comments regarding the game content or scenario** to facilitate comprehension of the storyline:

> *"We don't know that is what we are trying to find out?"* was provided in response to *"What happened to Sarah?"*

Similarly, a small number of police guides **provided cyber-safety advice** to students during game play, either related to the scenario, or relative to students' technology use outside of the game:

> *"We should never take someone at face value who we don't know!"*

Notably, very few police guides engaged in **general conversation** with students.

Volunteer guides

Volunteer guides are those organised by schools playing the CSD activity and may include teachers, IT specialists, education assistants, parents and older students. No data is collected by the ACMA as to the role of these volunteers within the school community. While schools are advised to provide one online guide for every 15 students playing the CSD

activity, this is not always possible within a school setting. Hence, the number of volunteer guides supporting facilitation of the CSD activity may be less than optimal. A large number of comments, 1,919, posted by guides in the evaluation period were posted by volunteer guides.

Many volunteer guides posted comments that **provided guidance** to students in playing the CSD activity (e.g., what do you think?) and to **prompt student to think critically** about how their learning in the CSD activity context applies to their own technology use:

"Why do you think your details are not safe?"

"Do you think that you could trust someone if you had only sent messages to them online, but never met?"

Approximately one quarter of responses offered by volunteer guides **provided reassurance and encouragement** for students in progressing through the game, while a small portion of the comments posted by volunteer guides comprised **general conversation** with students:

"Yes very good answer."

"Excellent detectives!"

"Hey cool cats hows it going?"

A few responses provided by volunteer guides included **cyber-safety advice** for students related to the CSD activity, but not specific to the game scenario:

"You need to be very careful about the information you share about yourself online."

A very small portion of volunteer guides provided responses to **answer students' questions about the game content or scenario**, facilitating students' comprehension of the storyline. For example, a student asked *"Where is Sarah"* to which the guide response was:

"That's what we need to find out."

Students who asked questions such as *"how long have u known Kel? Is the pic recently added?"* were provided responses similar to:

"None of us know Kel, we don't even know if the picture is really him."

As would be expected due to their lower familiarity with the CSD activity platform, very few volunteer guides responded to **students' questions about the game process** (e.g., how to find something). In addition, almost none of the volunteer guides posted comments that included their personal opinion about cyber-safety information or what to do in the CSD activity scenario.

Summary

The ACMA staff accounted for over half the comments posted by guides during CSD activity sessions between June and October. Volunteer guides were also very active in responding to students' comments, making up a large portion of the remaining comments by guides. The top three themes arising from the analyses identified guides responded to provide **reassurance and encouragement** to students, **provided guidance** to progress through the CSD activity, and responded to students to prompt them to **think critically**, usually to apply their learning to real life situations.

While some of the ACMA staff and volunteer guides engaged in **general conversation** with students, very few police guides posted comments of this nature. ACMA staff guides responded more often to **comments or questions about the game content or scenario** than did volunteer guides who more often **provided cyber-safety advice** to students.

Appendix 2: CSD activity modification suggestions

As a result of the data collected during this study, several suggestions are made for ways in which the impact and effectiveness of the game might be enhanced. Importantly, these suggestions should not be interpreted as a comment on the utility or applications of the game and are not intended to replace or diminish the results described in other sections of this report.

1. **Enhance student interaction:**
    a. Allow users to choose elements of gaming environment, for example, the colour scheme, character's gender.
    b. Allow users to choose avatars to represent their online team.
    c. Streamline the game platform to enable students to delete messages once read, or follow a chat script, rather than email-style communication, for ease of following the storyline and de-cluttering content.

2. **Increase data collection/quantitative input:**
    a. Formalise the polling questions, including refining their wording, and record this data.
    b. Allocate points to teams for each correct answer selected to meet students' expectations of a reward scheme within cyber-safety games.

3. **Enhance student engagement:**
    a. Update the environment/setting to include SNS.
    b. Present users with challenges/additional cyber-safety problems that are relevant but secondary to the game. For example, use the game as a means to raise issues of data sharing/retention/distribution and the management of digital reputation.

c. Develop a variety of scenarios that can be incorporated into the game. This will give users (teachers, etc.) a variety of options to choose from and will enable the game to be used multiple times with the same group or in consecutive years of schooling.

d. Construct scenarios in a developmental fashion where the challenges become increasingly personal in relation to the user's management of personal information/data.

4. Improve teacher information package:

a. Condense participation requirements to a one-page summary to ensure teachers read and understand what is involved in participating in the CSD activity.

b. Strengthen the emphasis placed on completing the pre- and post-game activities to reinforce and enhance students' comprehension of cyber-safety messages.

c. Ensure sufficient time is given to teachers to read the information package and conduct pre-game activities to prepare students for participation.

5. Role of guides:

a. Increase the involvement of police guides through the recruitment of ex-police staff, as students responded well to their involvement but police guides had low levels of student interaction in this study.

b. Train staff in community-based organisations related to cyber-safety to act as guides to alleviate the pressure on schools to find additional staff to support implementation and to provide more experts to respond to student messages.

6. Package the CSD activity as part of a suite of cyber-safety activities:

a. To reinforce cyber-safety messages and increase the likelihood of students transferring skills and strategies learnt through participation, the ACMA should consider offering schools a package of activities to complete with students. This package should include promotion of the CSD activity as part of series of activities, including Cybersmart Hero and the ACMA units of work for 11-12-year-old students.

Appendix 3: ACMA staff interview protocol

CYBERSMART DETECTIVES EVALUATION
CONFIDENTIAL ACMA STAFF INTERVIEW

Introduction

The purpose of today's interview is to collect information relating to your experience with the Cybersmart Detectives Game. I will be asking you a series of questions allowing you to describe your involvement with the game and previous cyber-safety training, including your perception of the game's strengths, weaknesses and limitations, if any. I will also be inviting you to explore your thoughts and opinions on what could be developed or improved in the Cybersmart Detectives Game.

We are limited to a 35 minute discussion today so I may move on to a new question if we have all the information required, however if you would like to add more information please don't hesitate to stop me.

As we will be relying on you to describe your involvement with and perceptions of Cybersmart Detectives, it is necessary for me to record the discussion to ensure I have an accurate record. Is it okay if I use a tape recorder to record our discussion?

Thank you.

Do you have any questions before we start?

1. **What is your involvement with Cybersmart Detectives?**

2. **Have you had cyber-safety training before your involvement with Cybersmart Detectives?**

YES/NO

a. If yes, what type? From whom/which organization?

b. If yes, how much?

c. If no, what was your background prior to Cybersmart Detectives?

d. What training have you received from the A.C.M.A. as part of your role with Cybersmart Detectives?

3. **What are your main tasks associated with Cybersmart Detectives?**

4. **What do you think are the main strengths of Cybersmart Detectives?**

5. **What do you think are the main limitations of Cybersmart Detectives?**

6. **What would you like to see developed or improved in the Cybersmart Detectives game?**

7. **Can you please talk me through the process of schools' involvement in CSD**?

8. **Any other information you want to share**?

Appendix 4: Stakeholder interview protocol

INDUSTRY STAKEHOLDER INTERVIEW

INTRODUCTION:

Hello

My name is _____ and I am from the Child Health Promotion Research Centre at Edith Cowan University. I'm calling to interview you as part of the evaluation we are conducting on the Australian Communications and Media Authority's Cybersmart Detectives game. Is this still a good time to conduct the interview?

No	**→ could we please arrange another time when I can call you back?**
Yes	**→ continue**

- **The purpose of today's discussion is to collect information about the design, content and implementation of a cyber-safety program for 11-12-year-old students and to discuss ACMA's Cybersmart Detectives game.**
- **I appreciate you are very busy so I will try to keep the interview to 15 mins.**
- **If it is okay with you, I would like to record our conversation today. This will help speed up the interview as I can listen to the tape and write notes once we have finished. It also allows me to collect an accurate record of your answers.**
- **Neither your name nor your organisation's name will be used in any reports arising from this research. Only aggregated responses will be described from all the interviews we are doing.**
- **Is this okay?**
- **Do you have any questions before we start?**

Questions:

1. **What support, if any, does your organisation currently provide to assist schools to address cyber-safety?**

_____

_____

2. **If you could develop strategies for schools to address cyber-safety, what would you include?**

[Interviewer to tick off the components identified. Prompt participant on any not listed, e.g. what about parent involvement?]

	✓
Establish a whole-school committee	
Policy development or review	
Promoting a respectful and caring school community	
Encouraging teachers to model the safe use of technology	
Professional development for school staff in using new technologies	
Cyber-safety curriculum materials	
Parents involvement (see prompt below)	
Local community involvement (see prompt below)	
Interactive, online game for students	
Online advertising about cyber-safety	
Internet filtering products	

Other: *[record any other strategies listed by participant, not included in list above]*

[prompt: How would you involve parents/or the local community]

_____

_____

_____

_____

3. **If you/your organisation were to develop a new cyber-safety educational activity for 11-12-year-old students, in what format would you deliver it (e.g. online, paper based, classroom curriculum)?**

_____

_____

[If participant says online:]
What would this online activity look like (i.e. what format would it take)?

_____

_____

[Prompt if participant does not mention game]
How useful would an online, interactive game be to communicate cyber-safety messages to this age group? Why/why not?

_____

_____

4. **If a resource, such as a game, were developed to deliver cyber-safety messages to 11-12-year-old students, how would you/your organisation promote it to schools?**

_____

_____

5. **In what ways would your organisation support schools in implementing a cyber-safety resource, such as a game, for 11-12-year-old students?**

[Prompt: newsletters, help desk, face-to-face training, web conference, grant funding, informative website, game instruction manual]

_____

_____

_____

6. **What do you see as being the most important cyber-safety messages to communicate to 11-12-year-old students?**

_____

_____

7. **What do you see as being the most effective strategies to communicate cyber-safety messages to 11-12-year-old students?**

_____

_____

8. **If a new cyber-safety game was developed for 11-12-year-old students, what do you consider will be the most important factors to address to <u>enhance the game's success</u>?**

_____

_____

9. **If a new cyber-safety game was developed for 11-12-year-old students, what do you think are likely to be the biggest <u>barriers affecting the game's success</u>?**

_____

_____

10. **If a new cyber-safety game was developed for 11-12-year-old students, what do you think are likely to be the biggest <u>barriers affecting implementation in schools</u>?**

_____

_____

11. **Could you please tell me your thoughts on the advantages/ disadvantages of online resources?**

_____

_____

Thank you very much for your time today. I just have two final questions to ask about you.

12. Which category best represents your age?

Under 25 years	25-29 years	30-34 years	35-39 years	40-44 years	45-49 years	50-54 years	55-59 years	60 years or older
1	2	3	4	5	6	7	8	9

13. What is your highest qualification?

Diploma	1
Bachelor degree	2
Post-grad Diploma / Masters	3
PhD	4
Other _____	5

14. That's all the questions I have to ask you. Is there anything else you would like to talk to me about that we haven't already covered?

_____

_____

Thanks again for your time ☺

15. [Interviewer to note gender]

Female	Male

Appendix 5: Data Collection Schedule

Monday	Tuesday	Wednesday	Thursday	Friday
30-Aug	31-Aug	1-Sep	2-Sep	3-Sep
			Eval School 01 9:30-10:30am (WST) **1 class, 31 students**	
6-Sep	7-Sep	8-Sep	9-Sep	10-Sep
Eval School 08 rescheduled	Eval School 03 11:20-12:20pm (WST) 1 class, 25 students *rescheduled*	**Eval School 12 10:00-11:00am (WST)** **1 class, 22 students**	**Eval School 07 11:30-12:30pm (WST)** **2 classes, 38 students**	
13-Sep	14-Sep	15-Sep	16-Sep	17-Sep
Eval School 05 9:45-10:45am (WST) 11:20-12:20am (WST) **2 classes, 58 students**	**School 01 post-test**	*Eval School 09 rescheduled*	**Eval School 06 9:30-10:30am (WST)** **1 class, 23 students** **Eval School 04 11:30-12:30pm (WST)** **2 classes, 52 students**	**Eval School 10 1:30-2:30pm (WST)** **1 class, 32 students**
20-Sep	21-Sep	22-Sep	23-Sep	24-Sep
School 05 post-test	**School 12 post-test**		**School 07 post-test** **School 06 post-test** **School 04 post-test**	**School 10 post-test**
School Holidays	School Holidays	School Holidays	School Holidays	School Holidays
18-Oct	19-Oct	20-Oct	21-Oct	22-Oct
Eval School 08 9.20-10:20pm (WST) 11.15-12:15pm (WST) **2 class, 56 students**	**Eval School 03 11:20-12:20pm (WST)** **1 class, 25 students**			
25-Oct	26-Oct	27-Oct	28-Oct	29-Oct
School 08 post-test	**School 03 post-test**			

Pre-test survey and CSD activity play day; *Games rescheduled* ; Post-test survey and teacher interview day

School 03 needed to reschedule their game session due to technical difficulties.
School 08 needed to be rescheduled due to classes with ACMA commitments during Child Protection Week.
School 09 needed to reschedule and thereafter cancel their game booking due to staff illness.

Appendix 5a: Parent information letter and consent form (active consent)

Child Health Promotion Research Centre
School of Exercise, Biomedical & Health Science
Edith Cowan University
Bradford Street
Mt Lawley WA 6050

Phone: (08) 9370 6350
Fax: (08) 9370 6511

PARENT INFORMATION LETTER
Educational Evaluation of Cybersmart Detectives

August 2010

Dear Parent/Carer

The Child Health Promotion Research Centre (CHPRC) at Edith Cowan University is conducting an evaluation to assess the effectiveness of the cyber-safety game - Cybersmart Detectives (CSD), on behalf of the Australian Communications and Media Authority (ACMA). Your son or daughter's school, School Name, was selected from all non-Government schools in Western Australia and has agreed to participate in this project. If the CSD is found to be effective it will do much to enhance the cyber-safety practices of young Australians. Ethics approval for this study has been provided by the Human Research Ethics Committee at Edith Cowan University.

What is the Cybersmart Detectives game?

Cybersmart Detectives (CSD) is an innovative online game that teaches children key Internet safety messages in a safe environment. Participants work online in real time liaising with community professionals to solve an Internet-themed problem. The activity is based in the school environment, and brings together a number of agencies with an interest in promoting online safety for young people, including State and Federal Police, education, government and child welfare advocates.

What does participation involve?

Your son or daughter's school will be participating in the CSD during Term 3, 2010. The game takes about 60 minutes to complete.

To evaluate the effectiveness of the game, we invite your son or daughter to complete ***two*** brief cyber-safety surveys. The **first** survey will take place on the same day as their participation in the CSD activity. The **second** survey will be conducted three weeks after participating in the CSD activity. Each survey will take approximately 15 minutes to complete and all responses provided will be treated as strictly confidential.

Your son or daughter may also be invited to participate in **one** focus group directly following their participation in the CSD activity. Focus group questions will ask about general perceptions of cyber-safety as well as more specific questions related to satisfaction with the CSD activity.

Your son or daughter's name will not be included in any reports resulting from this evaluation. All information collected from your son or daughter's school will also remain strictly confidential. All information will be stored securely (in locked cabinets and electronically in password protected files) at the CHPRC for at least five years before being destroyed. Participation in this study is voluntary. You and your son/daughter have the right to withdraw individual consent to participate in the evaluation at any time, without prejudice by contacting the Project Manager, Sarah Falconer on 9370 6803 or by email: s.falconer@ecu.edu.au.

Next steps:
1. Please complete the attached parent/carer consent form.
2. Please return the parent/carer consent form to the class teacher by Date.

Should you have any questions about your son or daughter's participation in the CSD evaluation, please do not hesitate to contact the Project Manager, Sarah Falconer at the Child Health Promotion Research Centre on 9370 6803 or by email: s.falconer@ecu.edu.au.

Yours sincerely

Dr Julian Dooley
Senior Research Fellow
Child Health Promotion Research Centre
Edith Cowan University, Western Australia

Cybersmart Evaluation - Parent/Carer Consent Form

This study has been approved by the Edith Cowan University Human Research Ethics Committee.

- I have been provided with a copy of the "Parent Information Letter", explaining the research project.
- I have read and understood the information provided.
- I have been given the opportunity to ask questions and have had any questions answered to my satisfaction.
- I am aware that if I have any additional questions I can contact the research team.
- I understand that participation in the Evaluation of Cybersmart Detectives will involve my son or daughter completing a short survey and that my son or daughter may be selected to participate in a focus group as part of the evaluation.
- I understand that the information provided will be kept confidential; that the identity of participants will not be disclosed without consent; and that all information will be securely stored for at least five years before being destroyed.
- I understand that the information provided will only be used for the purposes of this research project, and I understand how the information is to be used.
- I understand that my son/daughter's involvement is voluntary and my son/daughter can withdraw at any time without an explanation or penalty.
- I have discussed this research with my child, who has freely agreed to participate.

1. WRITTEN SURVEYS *(please tick one box only)*

☐ **I GIVE PERMISSION FOR** _____ (your son / daughter's name) to complete two confidential surveys for the Cybersmart evaluation. I have discussed this project with my son/daughter, who has also agreed to participate.

OR

☐ **I DO NOT GIVE PERMISSION FOR** _____ (your son / daughter's name) to complete two confidential surveys for the Cybersmart evaluation. I have discussed this project with my son/daughter, who has also agreed to participate.

2. FOCUS GROUP *(please tick one box only)*

☐ **I GIVE PERMISSION FOR** _____ (your son / daughter's name) to participate in one focus group for the Cybersmart evaluation. I have discussed this project with my son/daughter, who has also agreed to participate.

OR

☐ **I DO NOT GIVE PERMISSION FOR** _____ (your son / daughter's name) to participate in one focus group for the Cybersmart evaluation. I have discussed this project with my son/daughter, who has also agreed to participate.

Parent Name: _____ **School Name:** _____

Parent Signature: _____ **Date:** _____

Please return this form to the class teacher by X.

Appendix 5b: Parent information letter and consent form (passive consent)

Child Health Promotion Research Centre
School of Exercise, Biomedical & Health Science
Edith Cowan University
Bradford Street
Mt Lawley WA 6050

Phone: (08) 9370 6350

Fax: (08) 9370 6511

PARENT INFORMATION LETTER
Educational Evaluation of Cybersmart Detectives

August 2010

Dear Parent/Carer

As you may be aware, the Child Health Promotion Research Centre (CHPRC) at Edith Cowan University is conducting an evaluation to assess the effectiveness of the cyber-safety game - Cybersmart Detectives (CSD), on behalf of the Australian Communications and Media Authority (ACMA). Your son or daughter's school, School Name, was selected from all non-Government schools in Western Australia and has agreed to participate in this project. If the CSD is found to be effective it will do much to enhance the cyber-safety practices of young Australians. Ethics approval has been provided by the Human Research Ethics Committee at Edith Cowan University.

We have enclosed with this letter an ALTERNATIVE CONSENT FORM for your Year 6 son or daughter to participate in this project. This consent form seeks your permission for your son or daughter to participate in the evaluation of Cybersmart Detectives by completing the CSD activity during class time. They will also complete two confidential surveys during Term 3, 2010 and may be invited to participate in one focus group to discuss their general perceptions of cyber-safety as well as more specific questions related to satisfaction with the CSD activity. We are sending you this letter as we would like to give you another opportunity for your son or daughter to participate in this evaluation.
If you believe you have responded previously, please contact the Project Manager at the Child Health Promotion Research Centre, Sarah Falconer on (08) 9370 6803 or by email:s.falconer@ecu.edu.au.

What is the Cybersmart Detectives game?

Cybersmart Detectives (CSD) is an innovative online game that teaches children key Internet safety messages in a safe environment. Participants work online in real time liaising with community professionals to solve an Internet-themed problem. The activity is based in the school environment, and brings together a number of agencies with an interest in promoting online safety for young people, including State and Federal Police, education, government and child welfare advocates.

What does participation involve?

Your son or daughter's school will be participating in the CSD during Term 3, 2010. The game takes about 60 minutes to complete.

To best evaluate the effects of the game, we invite your son or daughter to complete ***two*** brief cyber-safety surveys. The **first** survey will take place on the same day as their participation in the CSD activity. The **second** survey will be conducted three weeks after participating in the CSD activity. Each survey will take approximately 15 minutes to complete and all responses provided will be treated as strictly confidential.

Your son or daughter may also be invited to participate in **one** focus group directly following their participation in the CSD activity. Focus group questions will ask about general perceptions of cyber-safety as well as more specific questions related to satisfaction with the CSD activity.

Next steps:

1. If you **WILL ALLOW** your Year 6 son or daughter to participate in the CSD activity and respond to two confidential surveys and/or one focus group during Terms 3, 2010; YOU DO NOT NEET TO TAKE ANY ACTION. Your son or daughter will be asked for his/her consent to participate in class.

2. If you **DO NOT WANT** your Year 6 son or daughter to participate in the CSD activity and respond to two confidential surveys and/or one focus group during Terms 3, 2010; please COMPLETE THE CONSENT FORM and return it to the class teacher by date. Your son or daughter will be provided with an alternative activity to complete while the surveys are being administered to other students in the class.

Your son or daughter's name will not be included in any reports resulting from this evaluation. All information collected from your son or daughter's school will also remain strictly confidential. All information will be stored securely (in locked cabinets and electronically in password protected files) at the CHPRC for at least five years before being destroyed. Participation in this study is voluntary. You and your son/daughter have the right to withdraw individual consent to participate in the evaluation at any time, without prejudice by contacting the Project Manager, Sarah Falconer on 9370 6803 or by email: s.falconer@ecu.edu.au.

Should you have any questions about your son or daughter's participation in the CSD evaluation, please do not hesitate to contact the Project Manager, Sarah Falconer at the Child Health Promotion Research Centre on 9370 6803 or by email: s.falconer@ecu.edu.au.

Yours sincerely

Dr Julian Dooley
Senior Research Fellow
Child Health Promotion Research Centre
Edith Cowan University, Western Australia

Cybersmart Evaluation - Parent/Carer Consent Form

This study has been approved by the Edith Cowan University Human Research Ethics Committee.

- I have been provided with a copy of the "Parent Information Letter", explaining the research project.
- I have read and understood the information provided.
- I have been given the opportunity to ask questions and have had any questions answered to my satisfaction.
- I am aware that if I have any additional questions I can contact the research team.
- I understand that participation in the Evaluation of Cybersmart Detectives will involve my son or daughter completing a short survey and that my son or daughter may be selected to participate in a focus group as part of the evaluation.
- I understand that the information provided will be kept confidential; that the identity of participants will not be disclosed without consent; and that all information will be securely stored for at least five years before being destroyed.
- I understand that the information provided will only be used for the purposes of this research project, and I understand how the information is to be used.
- I understand that my son/daughter's involvement is voluntary and my son/daughter can withdraw at any time without an explanation or penalty.
- I have discussed this research with my child, who has freely agreed to participate.

1. WRITTEN SURVEYS *(please tick one box only)*

☐ **I GIVE PERMISSION FOR** _____ (your son / daughter's name) to complete two confidential surveys for the Cybersmart evaluation. I have discussed this project with my son/daughter, who has also agreed to participate.

OR

☐ **I DO NOT GIVE PERMISSION FOR** _____ (your son / daughter's name) to complete two confidential surveys for the Cybersmart evaluation. I have discussed this project with my son/daughter, who has also agreed to participate.

2. FOCUS GROUP *(please tick one box only)*

☐ **I GIVE PERMISSION FOR** _____ (your son / daughter's name) to participate in one focus group for the Cybersmart evaluation. I have discussed this project with my son/daughter, who has also agreed to participate.

OR

☐ **I DO NOT GIVE PERMISSION FOR** _____ (your son / daughter's name) to participate in one focus group for the Cybersmart evaluation. I have discussed this project with my son/daughter, who has also agreed to participate.

Parent Name: _____ **School Name:** _____

Parent Signature: _____ **Date:** _____

Please return this form to the class teacher by X.

Appendix 6: Student surveys

6.1 Pre-test survey

CYBERSMART DETECTIVES PROJECT

CONFIDENTIAL SURVEY

Dear Student

We are using this survey to find out your thoughts on cyber-safety. In this survey, we will be asking you some questions about yourself and your experiences with the Internet and mobile phones. When you answer the questions please think about things that happen when you are on the Internet or while using your mobile phone.

All the information you provide will remain confidential. No one at your school or your home will see your answers. Your answers will be stored on an external server accessible only by the researchers.

This is not a test, there are no right or wrong answers. Please answer all the questions as honestly as you can. We are very interested in what you have to say and not what others around you think. If you have any questions, please ask the researchers and NOT your teacher or other students.

If you don't want to answer any questions, you don't have to and if you do not want to complete this survey you do not have to.

Thank you for your help.

Dr Julian Dooley
Child Health Promotion Research Centre
Edith Cowan University, Western Australia

1. What is your age in years today?
(please write your age in the boxes below)

Years

2. Are you male or female?
*(please circle **ONE NUMBER** only)*

Male	1
Female	2

3. Who do you live with MOST of the time?
*(please circle **ONE NUMBER** only)*

Both parents	1
Mother and stepfather / other adult male	2
Father and stepmother / other adult female	3
Mother only	4
Father only	5
I am a boarder	6
Other guardian	7

4. What is your home postcode?

The next few questions ask about your use of the Internet and mobile phones.

5. Do you:
*(please circle **ONE NUMBER for each** statement)*

		Yes	No
a	have your own mobile phone?	1	2
b	have Internet access on your mobile phone?	1	2
c	have Internet access at home?	1	2
d	have wireless Internet access at home?	1	2
e	use the Internet on a computer or laptop in your bedroom?	1	2
f	have a social networking site (e.g. MySpace, Facebook, Club Penguin)?	1	2
g	use an instant messaging program (e.g. MSN, Yahoo!Chat)?	1	2
h	use a webcam?	1	2

6. In total how many <u>calls</u> do you <u>get and make</u> on your mobile phone:
*(please circle **ONE NUMBER for each** statement)*

		I don't have a mobile phone	None	1-3 calls a day	4-5 calls a day	6-10 calls a day	More than 10 calls a day
a	on an average day at school?	1	2	3	4	5	6
b	on an average day before or after school?	1	2	3	4	5	6
c	on an average day on the weekend?	1	2	3	4	5	6

7. How many <u>text messages</u> (SMS) **do you <u>send</u> on your mobile phone:**
*(please circle **ONE NUMBER for each** statement)*

		I don't have a mobile phone	Less than 5	6-10	11-15	16-20	More than 20
a	on an average day at school?	1	2	3	4	5	6
b	on an average day before or after school?	1	2	3	4	5	6
c	on an average day on the weekend?	1	2	3	4	5	6

8. How many times a day do you use the Internet on your mobile phone (e.g. to download ring tones, play games, use your social networking site, or chat)**:**

*(please circle **ONE NUMBER for each** statement)*

		I don't have a mobile phone	None	1-3 times a day	4-5 times a day	6-10 times a day	More than 10 times a day
a	on an average day at school?	1	2	3	4	5	6
b	on an average day before or after school?	1	2	3	4	5	6
c	on an average day on the weekend?	1	2	3	4	5	6

9. For how many hours each day in total do you use the Internet?

*(please circle **ONE NUMBER for each** statement)*

		I don't use the Internet	Less than 1 hour	About 1 hour	About 2 hours	About 3 hours	About 4 hours	More than 4 hours
a	on an average week day for school work?	0	1	2	3	4	5	6
b	on an average week day NOT for school work?	0	1	2	3	4	5	6
c	on an average day on the weekend for school work?	0	1	2	3	4	5	6
d	on an average day on the weekend NOT for school work?	0	1	2	3	4	5	6

10. Where do you usually use the Internet?

(please circle as many as apply)

I do not use the Internet	1
At home	1
At school	1
At a friends' house	1
At the library	1
Other (please specify) _____	1

11. At home, where do you usually use the Internet?

(please circle as many as apply)

I do not use the Internet at home	1
In an open area (e.g. lounge room, family room, kitchen)	1
In my bedroom	1
In the study or separate room	1
In the bathroom	1
Other (please specify) _____	1

12. Do you use a social networking site (e.g. Facebook, MySpace, Club Penguin) **or instant messenger** (e.g. MSN)**?**

Yes	1
No	2
Unsure	3

13. Which social networking page / instant messenger do you use?

(please circle as many as apply)

I do not use a social networking site / instant messenger	1
Club Penguin	1
Bebo	1
MySpace	1
Facebook	1
MSN	1
Twitter	1
Others (please specify all / as many as you use) _____	1

14. For how many hours do you use a social networking site and / or instant messaging site (e.g. MySpace, Facebook, Club Penguin, MSN)**:**

*(please circle **ONE NUMBER for each** statement)*

		I don't have this	Less than half an hour	About half an hour	About 1 hour	About 2 hours	About 3 hours	4 hours or more
a	on an average day at school?	1	2	3	4	5	6	7
b	on an average day before or after school?	1	2	3	4	5	6	7
c	on an average day on the weekend?	1	2	3	4	5	6	7

15. Which of the following things have you done?

*(please circle **ONE NUMBER for each** statement)*

		No	Yes	I don't use social networking sites
a	I only have online friends that I have met in person?	1	2	3
b	I have set my profile to private?	1	2	3
c	I have shared my password with others?	1	2	3
d	I have blocked or deleted someone who said something I think is rude or mean?	1	2	3
e	I have not shared my personal details (e.g. mobile phone number, home or email address) with anyone?	1	2	3
f	I let my parents/caregivers know who is on my friends list?	1	2	3

16. How many friends or contacts do you have on your Facebook / MySpace / Club Penguin / Instant Messenger?

Please choose the highest number of friends / contacts that you have on ONE of these sites.

*(please circle **ONE NUMBER** only)*

a	I don't have any of these accounts	1
b	0-19	2
c	20-49	3
d	50-99	4
e	100-149	5
f	150-199	6
g	200-299	7
h	300 or more	8

17. How many of these friends do you know in person (e.g. friends at school or outside of school)**?**

*(please circle **ONE NUMBER** only)*

I don't have/use this	None	About half	Nearly all	All
1	2	3	4	5

18. Do you use chat sites on the Internet?

Yes	1
No	2
Unsure	3

19. Please write the name/s of the Internet chat site(s) you use in the table below.
Then, circle how much time you usually spend in each chat site.

		I do not use Internet chat sites	**I usually spend:** **Less than 15 minutes** in this chat site	**About 30 minutes** in this chat site	**About 45 minutes** in this chat site	**About 1 hour** in this chat site	**More than 1 hour** in this chat site
a	Internet chat site 1: _____	1	2	3	4	5	6
b	Internet chat site 2: _____	1	2	3	4	5	6
c	Internet chat site 3: _____	1	2	3	4	5	6

20. Do you play games on the Internet (e.g. WoW – World of Warcraft)**?**

Yes	1
No	2
Unsure	3

21. If yes, what do you play online games with?
(please circle as many as apply)

I do not play online games	1
Nintendo DSi	1
PlayStation Portable (PSP)	1
PlayStation (e.g. PS2, PS3)	1
Xbox	1
Computer (e.g. a laptop or home computer)	1
Others (please name as many as you use) _____	1

22. When you play online games, do you play with:
*(please circle **ONE NUMBER** only)*

ONLY people you have met in person	1
ONLY people you have never met	2
BOTH people you know in person and people you have never met	3
I don't play games online with any other person	4
I don't play online games	5

You are doing a great job!

*The next few questions ask your experiences **on** your computer/mobile phone (online)*

*and **off** your computer/mobile phone (offline).*

23. Have you ever been contacted online by someone you have not met in person: *(please circle **ONE NUMBER for each** statement)*

		I don't have or don't use	Never	Only 1 time	2-3 times	4-5 times	More than 5 times
a	on your social networking site (e.g. Facebook, MySpace, Club Penguin)?	1	2	3	4	5	6
b	on instant messenger like MSN?	1	2	3	4	5	6
c	on your webcam?	1	2	3	4	5	6
d	on your mobile phone?	1	2	3	4	5	6
e	in a chatroom?	1	2	3	4	5	6
f	on your blog?	1	2	3	4	5	6
g	in an online game?	1	2	3	4	5	6
h	other (please describe): _____	1	2	3	4	5	6

24. If you were contacted on your mobile phone, an online game, an online chat site or when using a social networking site by someone you don't know, what would you do?

*(please circle **ONE NUMBER for each** statement)*

		No	Yes
a	I would not respond to the messages	2	3
b	I would leave the chat session or log out immediately	2	3
c	I would block the person who contacted me	2	3
d	I would keep the messages/chat as evidence	2	3
e	I would talk to a parent about it	2	3
f	I would talk to a teacher/principal about it	2	3
g	I would talk to the police about it	2	3
h	I would talk to a friend about it	2	3
i	I would talk to other family members about it	2	3
j	I would talk to my Internet Service Provider (e.g. Telstra, Optus) about it	2	3
k	I would talk to someone else about it (e.g. Kids Helpline), please describe who you would talk to: _____	2	3
l	I would set my social network profile to private	2	3
m	I would make sure not to open any messages or emails that the person I don't know sent me	2	3
n	Other: _____	2	3

25. Please list your favourite three websites and circle how often you visit each.

		I visit this website **about once a month**	I visit this website **about once a week**	I visit this website **every 2-3 days**	I visit this website **once a day or more**
a	Website 1: _____	1	2	3	4
b	Website 2: _____	1	2	3	4
c	Website 3: _____	1	2	3	4

DONE!

Thank you for completing this survey.

If answering questions in this survey raises any issues or feelings that concern you please talk to an adult you trust (e.g. parent, school counsellor, school nurse, or social worker).

You can also phone the Kids Help Line.

They provide a free, confidential, anonymous 24-hour telephone and online counselling service for young people aged between 5 and 18 years. You teacher will hand out a leaflet with further information.

6.2 Post-test survey

CYBERSMART DETECTIVES PROJECT

CONFIDENTIAL SURVEY

Dear Student

We are using this survey to ask you some questions about the Cybersmart Detectives game that you recently played. We would also like to ask you some questions about staying safe on the Internet. This survey is short and will only take about 10 minutes to answer all the questions.

All the information you provide will remain confidential. No one at your school or your home will see your answers.

This is not a test, there are no right or wrong answers. Please answer all the questions as honestly as you can. We are very interested in what you have to say and not what others around you think. If you have any questions, please ask the researchers and NOT your teacher or other students.

If you don't want to answer any questions, you don't have to and if you don't want to complete this survey you don't have to.

Thank you for your help.

Dr Julian Dooley

Child Health Promotion Research Centre

Edith Cowan University, Western Australia

1. **These questions ask about the Cybersmart Detectives game that you played recently.** *(please circle **ONE NUMBER for each** statement)*

a	How old was the girl in the story?	I don't remember	13 years	14 years	15 years
b	Who had been contacting her?	I don't remember	Tel15	Kel17	Tim16
c	What was Sarah's hobby in the story?	I don't remember	Roller blading	Biking	Running
d	How did the boy get Sarah's mobile number?	I don't remember	She gave it to him	They had friends in common	He got it online
e	Where did the boy want to take Sarah?	I don't remember	His house	Local skate park	To the cinema
f	Where is Sarah's computer at home?	I don't remember	In her bedroom	In the family room	She does not have one at home
g	How old was the person waiting for Sarah at the school gate?	I don't remember	17 years	37 years	21 years
h	Were the police called?	I don't remember	Yes	No	

2. **Which of the following things have you done?**
*(please circle **ONE NUMBER for each** statement)*

		I don't use social networking sites	**No**	**Yes**
a	I only have online friends that I have met in person?	1	2	3
b	I have set my social networking site profile to private?	1	2	3
c	I have shared my password with others?	1	2	3
d	I have blocked or deleted someone who said something I think is rude or mean?	1	2	3
e	I have not shared my personal details (e.g. mobile phone number, home or email address) with anyone?	1	2	3
f	I let my parents/caregivers know who is on my friends list?	1	2	3

*The next few questions ask your experiences **on** your computer/mobile phone (online)*

*and **off** your computer/mobile phone (offline).*

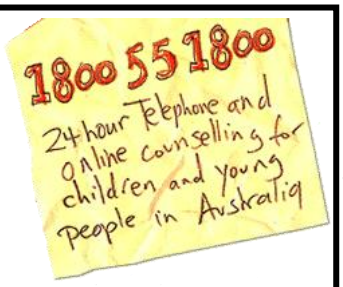
3. Have you ever been contacted online by someone you have not met in person: *(please circle **ONE NUMBER for each** statement)*

		I don't have or don't use	Never	Only 1 time	2-3 times	4-5 times	More than 5 times
a	on your social networking site (e.g. Facebook, MySpace, Club Penguin)?	1	2	3	4	5	6
b	on instant messenger like MSN?	1	2	3	4	5	6
c	on your webcam?	1	2	3	4	5	6
d	on your mobile phone?	1	2	3	4	5	6
e	in a chatroom?	1	2	3	4	5	6
f	on your blog?	1	2	3	4	5	6
g	in an online game?	1	2	3	4	5	6
h	other (please describe): _____	1	2	3	4	5	6

4. If you were contacted on your mobile phone, an online game, an online chat site or when using a social networking site by someone you don't know, what would you do? *(please circle **ONE NUMBER for each** statement)*

		No	Yes
a	I would not respond to the messages	2	3
b	I would leave the chat session or log out immediately	2	3
c	I would block the person who contacted me	2	3
d	I would keep the messages/chat as evidence	2	3
e	I would talk to a parent about it	2	3
f	I would talk to a teacher/principal about it	2	3
g	I would talk to the police about it	2	3
h	I would talk to a friend about it	2	3
i	I would talk to other family members about it	2	3
j	I would talk to my Internet Service Provider (e.g. Telstra, Optus) about it	2	3
k	I would talk to someone else about it (e.g. Kids Helpline), please describe who you would talk to: _____	2	3
l	I would set my social network profile to private	2	3
m	I would make sure not to open any messages or emails that the person I don't know sent me	2	3
n	Other: _____	2	3

Thank you for completing this survey. You can also phone the Kids Help Line. They provide a free, confidential, anonymous 24-hour telephone and online counselling service for young people aged between 5 and 25 years.



Appendix 7. Frequency and type of website visited

Website	n	% of students (n=292)	Once/month	Once/week	Every 2-3 days	Once/day or more
Facebook	91	31	7	13	34	46
MSN	75	26	8	25	39	28
YouTube	44	15	20	30	34	16
Club Penguin	36	12	47	33	8	11
Hotmail/ Yahoo/ Gmail	30	10	20	27	27	27
Google	28	10	11	11	29	50
Miniclip	18	6	44	22	28	6
Cool maths games	16	5	6	44	44	6
Moshi Monsters	14	5	29	36	21	14
Mathletics	12	4	8	75	8	8
Addicting games	9	3	33	44	11	11
Class Wiki	8	3	25	12	38	25
Friv	8	3	62	38	0	0
Skype	8	3	12	50	25	12
Stardoll	8	3	12	0	88	0
Runescape	7	2	14	14	43	29
MySpace	6	2	50	33	17	0
Armor games	5	2	40	20	20	20
iTunes	5	2	0	60	20	20
Fan Fiction	5	2	0	0	0	100

Call of Duty	4	1	0	25	0	75
Habbo Hotel	4	1	50	0	0	50
Superpokepets / Neopets	4	1	0	25	25	50
Wikipedia	4	1	50	50	0	0
World of Warcraft	4	1	0	50	0	50
Bloons	3	1	0	100	0	0
Funorb	3	1	0	33	67	0
Lego Network	3	1	0	0	33	67
Poptropica	3	1	33	33	33	0
Twitter	3	1	0	67	33	0
A-game	2	1	0	0	50	50
Blogspot	2	1	0	50	50	0
Bored	2	1	0	0	0	100
Combat arms	2	1	0	0	0	100
Fantage	2	1	0	50	50	0
Free Pacman	2	1	0	50	50	0
Fun school	2	1	50	50	0	0
Games games	2	1	0	50	0	50
Girlgames.com	2	1	50	50	0	0
Girlsgogames	2	1	0	50	50	0
Library	2	1	0	50	50	0
Maths online	2	1	0	50	50	0
Nexon	2	1	0	0	50	50
Ninjagames.com / Ninja Kiwi	2	1	50	0	50	0

One more level	2	1	0	0	50	50
PlayStation Network	2	1	0	50	0	50
Spelling city	2	1	0	50	0	50
Stick page/ Stick game	2	1	0	50	50	0
Youda Sushi Chef	2	1	100	0	0	0
Allycarter.com	1	1	0	100	0	0
Arcad street	1	1	100	0	0	0
Banana games	1	1	0	100	0	0
Battlefield	1	1	0	0	100	0
Bebo	1	1	100	0	0	0
Bloxors	1	1	0	100	0	0
Bubbleboxgames.com	1	1	0	100	0	0
Camino	1	1	100	0	0	0
Car games	1	1	0	100	0	0
Choleneill.com	1	1	0	0	0	100
CIA	1	1	0	100	0	0
Cool fun games	1	1	0	0	100	0
Conspiracy365.com.au	1	1	0	100	0	0
Counterstrike online	1	1	0	0	100	0
Disney	1	1	100	0	0	0
Dizzywood	1	1	100	0	0	0
eBay	1	1	100	0	0	0
Ebday	1	1	0	100	0	0
Ebgames	1	1	0	100	0	0

Fielders choice	1	1	100	0	0	0
Flash games	1	1	0	0	0	100
Football West	1	1	0	100	0	0
Footy Tips	1	1	0	0	100	0
Foxsports	1	1	0	100	0	0
Free math games	1	1	0	100	0	0
Free Rider	1	1	0	100	0	0
Free world group	1	1	0	100	0	0
Funny games	1	1	0	100	0	0
Game bong	1	1	0	0	100	0
Game freaks	1	1	100	0	0	0
Gamenode	1	1	100	0	0	0
Gamespot.com	1	1	0	0	100	0
Games 4 girls	1	1	0	0	0	100
Games 2 win	1	1	100	0	0	0
Halo Live	1	1	0	0	0	100
Horseisle	1	1	0	0	100	0
i-dressup	1	1	0	0	0	100
JonasBrothers Australia.com	1	1	100	0	0	0
Justin Bieber	1	1	0	0	0	100
Kitbag	1	1	0	100	0	0
Kongregate	1	1	0	100	0	0
Learn to fly	1	1	100	0	0	0
Lyrics.com	1	1	0	100	0	0

Mangafox	1	1	0	100	0	0
Maple story	1	1	0	0	0	100
Mathlites	1	1	0	100	0	0
Metro modelling	1	1	0	100	0	0
Mincecraft	1	1	100	0	0	0
MissGuffie.com.au	1	1	0	100	0	0
Mug tug	1	1	0	0	100	0
Optical illusions	1	1	0	0	0	100
Oynular 1	1	1	0	100	0	0
New grounds	1	1	0	0	0	100
News	1	1	100	0	0	0
Penguinz	1	1	100	0	0	0
Perth Zoo	1	1	0	100	0	0
Plus 7	1	1	0	100	0	0
Ponywood	1	1	0	100	0	0
Primary games	1	1	100	0	0	0
Prodirect	1	1	0	100	0	0
Puff games	1	1	100	0	0	0
Random Mando	1	1	100	0	0	0
Rubble Trouble	1	1	0	100	0	0
Safari	1	1	100	0	0	0
School’s website	1	1	0	100	0	0
Scootle	1	1	0	100	0	0
Skater HQ	1	1	100	0	0	0

Skysports	1	1	0	0	0	100
Soccer Bible	1	1	0	0	0	100
Steam	1	1	0	0	0	100
Street sesh	1	1	100	0	0	0
Super secret	1	1	0	0	100	0
Tankspot	1	1	0	0	0	100
The Sims	1	1	0	0	0	100
Total girl	1	1	100	0	0	0
Twilight games	1	1	0	100	0	0
Two player games	1	1	100	0	0	0
Watchtv.ten.com.au	1	1	100	0	0	0
www.y8.com	1	1	100	0	0	0
Zefron.com	1	1	100	0	0	0
39Clues	1	1	0	0	100	0

Appendix 8. Student quantitative results by gender

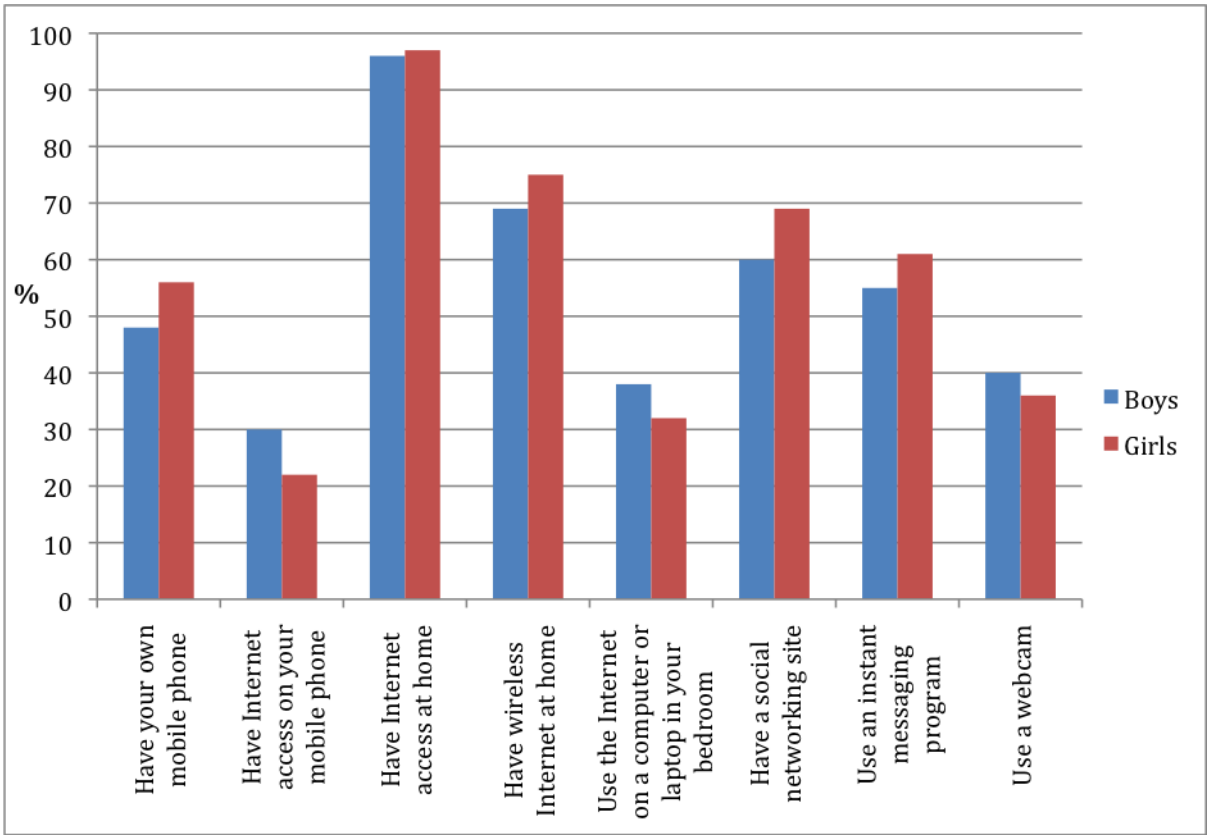
Technology use

Students were asked a series of questions relating to their technology use. First, students were asked about their access to technology (Table 54, Figure 17). Approximately half (Boys: 48%, *n* = 56; Girls: 56%, *n* = 92) of the students surveyed reported they have their own mobile phone, with some students having Internet access on their mobile phone (Boys: 30%, *n* = 35; Girls: 22%, *n* = 36). Almost all students reported having access to the Internet at home (Boys: 96%, *n* = 112; Girls: 97%, *n* = 156) and for the majority, this access was available wirelessly (Boys: 69%, *n* = 80; Girls: 75%, *n* = 118). Interestingly, approximately one-third of students (Boys: 38%, *n* = 45; Girls: 32%, *n* = 53) reported they use the Internet on a computer or laptop in their bedroom. When asked about their social contact on the Internet, approximately two-thirds of students reported having a social networking site (Boys: 60%, *n* = 70; Girls: 69%, *n* = 113) whereas approximately half of students reported they use an instant messaging program (Boys: 55%, *n* = 64; Girls: 61%, *n* = 100) and between one-third and two-fifths of students reported using a webcam (Boys: 40%, *n* = 47; Girls: 36%, *n* = 59).

Table 54. Students' technology use by gender

	Boys		Girls	
	Yes % (*n*)	**No** % (*n*)	**Yes** % (*n*)	**No** % (*n*)
Have your own mobile phone	48 (56)	52 (61)	56 (92)	44 (71)
Have Internet access on your mobile phone	30 (35)	70 (80)	22 (36)	78 (126)
Have Internet access at home	96 (112)	4 (5)	97 (156)	3 (5)
Have wireless Internet at home	69 (80)	31 (36)	75 (118)	25 (39)
Use the Internet on a computer or laptop in your bedroom	38 (45)	62 (72)	32 (53)	68 (110)
Have a social networking site	60 (70)	40 (47)	69 (113)	31 (50)
Use an instant messaging program	55 (64)	45 (53)	61 (100)	39 (63)
Use a webcam	40 (47)	60 (70)	36 (59)	64 (104)

Figure 17. Students' technology use by gender

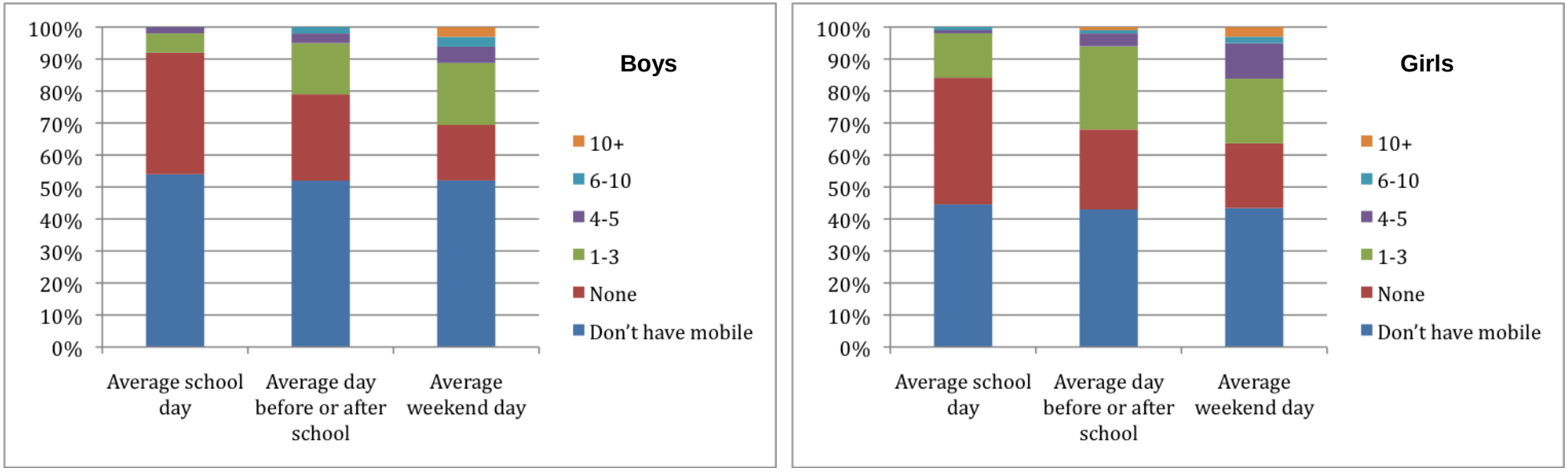


Students were then asked about the frequency with which they made and received phone calls (Table 55, Figure 18) and sent text messages on an average school day, before and after school and on the weekend (Table 56, Figure 19). Just over half of boys reported they do not have a mobile phone (55%, *n* = 61), whereas just under half of girls do not have a mobile phone (45%, *n* = 72). Of those who do, about one-third of students reported they did not receive or make any phone calls on an **average day at school** (Boys: 38%, *n* = 43; Girls: 40%, *n* = 64), followed by one to three calls per day (Boys: 6%, *n* = 7; Girls: 14%, *n* = 23). Approximately one-quarter of students reported they made or received no phone calls on an **average day before or after school** (Boys: 27%, *n* = 31; Girls: 25%, *n* = 40), with a similar number of students reporting they made or received between one and three phone calls (Boys: 16%, *n* = 18; Girls: 26%, *n* = 42) during this time period. One-fifth of students reported making or receiving no phone calls per day on an **average day of the weekend** (Boys: 17%, *n* = 20; Girls: 20%, *n* = 32) and a similar number reported they made or received between one and three phone calls (Boys: 19%, *n* = 22; Girls: 20%, *n* = 32) in this period of time.

Table 55. Frequency of calls made and received on students' mobile phone by gender

	Boys % (*n*)						Girls % (*n*)					
	Don't have mobile	None	1-3 times	4-5 times	6-10 times	10+ times	Don't have mobile	None	1-3 times	4-5 times	6-10 times	10+ times
Average school day	54 (61)	38 (43)	6 (7)	2 (2)	0 (0)	0 (0)	45 (72)	40 (64)	14 (23)	1 (1)	1 (1)	0 (0)
Average day before or after school	52 (60)	27 (31)	16 (18)	3 (4)	2 (2)	0 (0)	43 (70)	25 (40)	26 (42)	4 (7)	1 (1)	1 (2)
Average weekend day	51 (59)	17 (20)	19 (22)	5 (6)	3 (4)	3 (4)	43 (70)	20 (32)	20 (32)	11 (18)	2 (4)	3 (5)

Figure 18. Frequency of calls made and received on students' mobile phone by gender

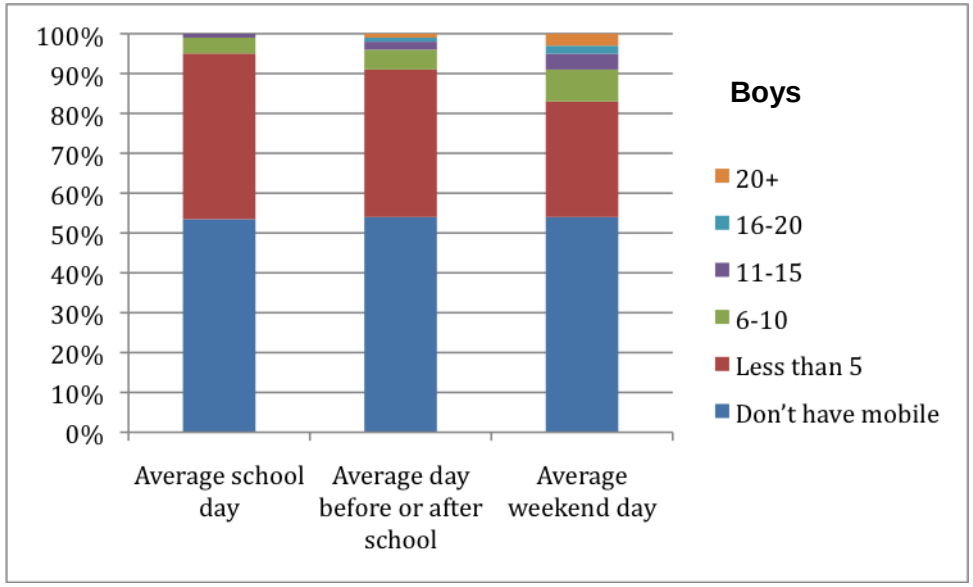


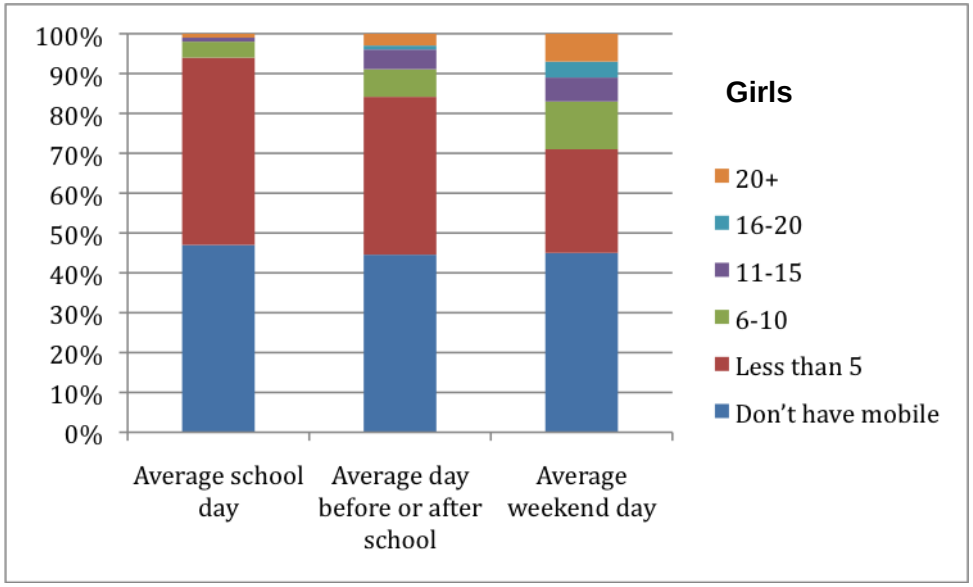
When asked about the frequency with which they sent text messages, again, the majority of boys reported they did not have a mobile phone (54%, *n* = 60) while 47% (*n* = 76) of girls reported this (Table 56, Figure 19). The majority of students reported sending less than five text messages on their mobile phone on an average day at school (Boys: 42%, *n* = 47; Girls: 47%, *n* = 77). On an average day before or after school, over one-third of students reported sending less than five text messages on their mobile phone (Boys: 37%, *n* = 42; Girls: 40%, *n* = 65), followed by between six and 10 text messages (Boys 5%, *n* = 6; Girls: 7%, *n* = 11) and 11 to 15 text messages (Boys: 2%, *n* = 2; Girls: 5%, *n* = 8). Responses to the question about text message use on an average day on the weekend were more varied. Just over one-quarter of students reported they send less than five text messages on an average day on the weekend (Boys: 29%, *n* = 33; Girls: 26%, *n* = 43), while 8% (*n* = 9) of boys and girls (12%, *n* = 20) reported sending between six and 10 text messages, 4% (*n* = 5) of boys and 6% (*n* = 9) of girls reported sending 11 to 15 text messages and 3% (*n* = 3) of boys and 7% (*n* = 11) of girls reported sending more than 20 text messages on an average day of the weekend.

Table 56. Frequency of text messages sent on students' mobile phone by gender

	Boys % (*n*)						Girls % (*n*)					
	Don't have mobile	Less than 5	6-10	11-15	16-20	20+	Don't have mobile	Less than 5	6-10	11-15	16-20	20+
Average school day	54 (60)	42 (47)	4 (4)	1 (1)	0 (0)	0 (0)	47 (76)	47 (77)	4 (6)	1 (1)	0 (0)	1 (2)
Average day before or after school	54 (60)	37 (42)	5 (6)	2 (2)	1 (1)	1 (1)	45 (73)	40 (65)	7 (11)	5 (8)	1 (1)	3 (5)
Average weekend day	54 (61)	29 (33)	8 (9)	4 (5)	2 (2)	3 (3)	45 (73)	26 (43)	12 (20)	6 (9)	4 (6)	7 (11)

Figure 19. Frequency of text messages sent on students' mobile phone by gender





Students were next asked how many times a day they used the Internet on their mobile phone (Table 57, Figure 20). Of the 47% of boys and 56% of girls who have a mobile phone, the majority of students reported they did not use the Internet on their mobile phone on an **average day at school**, with 6% (*n* = 7) of boys and 10% (*n* = 16) of girls reporting they used the Internet on their mobile phone one to three times. Again, the majority of students reported they did not have a mobile phone or that they did not use the Internet on their mobile phone on an **average day before and after school** and 10% (*n* = 11) of boys and 11% (*n* = 18) of girls reported using the Internet on their mobile phone between one and three times in this time period. Finally, 14% (*n* = 16) of boys and 9% (*n* = 14) of girls reported using the Internet on their mobile phone between one and three times on an **average day of the weekend**.

Finally, students were asked to describe their Internet use on an average weekday and an average day of the weekend, for schoolwork and not for schoolwork (Table 58, Figure 21). About two-fifths of students reported using the Internet for less than one hour on an **average week day for school work** (Boys: 48%, *n* = 56; Girls: 38%, *n* = 61), with about one-third of students (Boys: 31%, *n* = 36; Girls: 35%, *n* = 56) reporting they use the Internet for about an hour for school work on an average day of the week. When asked about the time spent using the Internet **on an average day of the week not for school work**, approximately one-third reported spending less than one hour (Boys: 30%, *n* = 34; Girls: 32%, *n* = 51) and a further one-third reported spending about an hour (Boys: 34%, *n* = 40; Girls: 28%, *n* = 44).

Just under half of students reported using the Internet for less than one hour on an **average day of the weekend for school work** (Boys: 49%, *n* = 56; Girls: 38%, *n* = 60), followed by about one hour (Boys: 23%, *n* = 27; Girls: 32%, *n* = 52), two hours (Boys: 10%, *n* = 12; Girls: 12%, *n* = 20) and three hours (Boys: 3%, *n* = 3; Girls: 7%, *n* = 11). Students' report of Internet use on an **average day of the weekend not for school work** was more varied than responses to other time use questions. Approximately one-fifth of students reported each of the following: less than one hour (Boys: 19%, *n* = 22; Girls: 21%, *n* = 34), about one hour (Boys: 21%, *n* = 24; Girls: 24%, *n* = 38) and about two hours (Boys: 23%, *n* = 27; Girls: 19%, *n* = 31), while 11% (*n* = 13) of boys and 13% (*n* = 21) of girls reported using the Internet for about three hours, 3% (*n* = 4) of boys and 6% (*n* = 10) of girls for about four hours and 17% (*n* = 20) of boys and 4% (*n* = 7) of girls for more than four hours on an average day of the weekend not for school work.

Table 57. Frequency of Internet use on students' mobile phone by gender

	Boys % (*n*)						Girls % (*n*)					
	Don't have mobile	None	1-3 times	4-5 times	6-10 times	10+ times	Don't have mobile	None	1-3 times	4-5 times	6-10 times	10+ times
Average school day	53 (59)	38 (42)	6 (7)	0 (0)	1 (1)	2 (2)	44 (71)	46 (75)	10 (16)	0 (0)	0 (0)	0 (0)
Average day before or after school	50 (57)	33 (37)	10 (11)	3 (3)	2 (2)	3 (3)	44 (71)	41 (66)	11 (18)	3 (5)	1 (1)	1 (1)
Average weekend day	52 (59)	23 (26)	14 (16)	4 (5)	1 (1)	5 (6)	43 (70)	35 (57)	9 (14)	7 (12)	4 (6)	2 (3)

Figure 20. Frequency of Internet use on students' mobile phone by gender

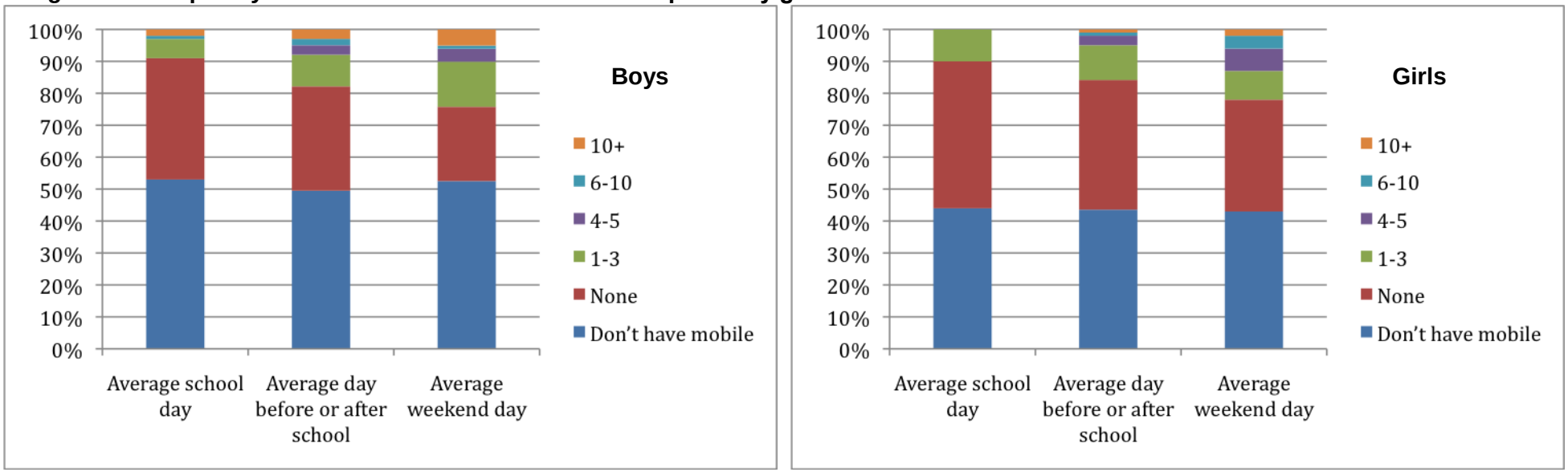
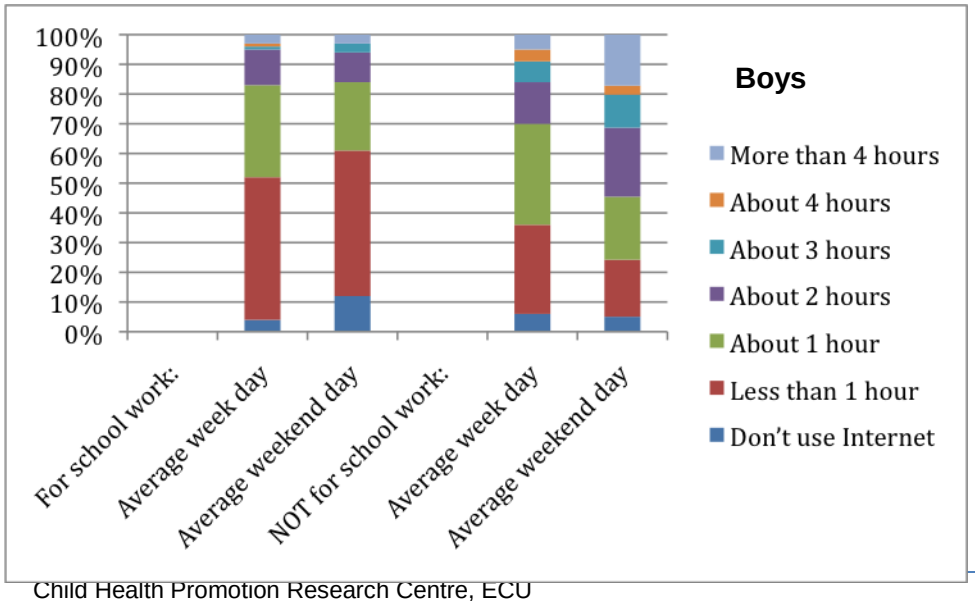
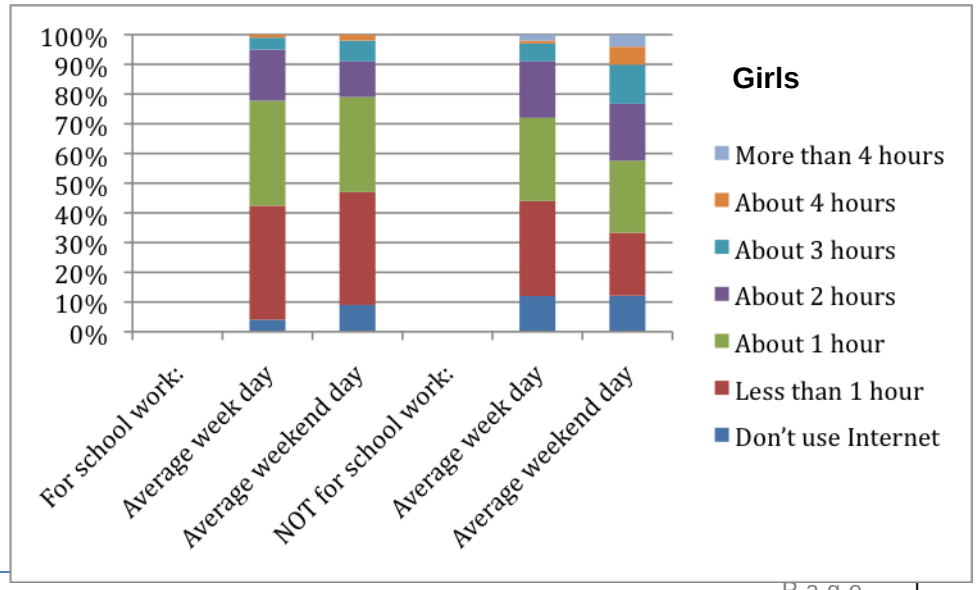


Table 58. Frequency of students' Internet use by gender

	Boys % (*n*)							Girls % (*n*)						
% (n)	Don't use Internet	Less than 1 hour	About 1 hour	About 2 hours	About 3 hours	About 4 hours	More than 4 hours	Don't use Internet	Less than 1 hour	About 1 hour	About 2 hours	About 3 hours	About 4 hours	More than 4 hours
For school work:														
Average week day	4 (5)	48 (56)	31 (36)	12 (14)	1 (1)	1 (1)	3 (3)	4 (7)	38 (61)	35 (56)	17 (27)	4 (6)	1 (2)	0 (0)
Average weekend day	12 (14)	49 (56)	23 (27)	10 (12)	3 (3)	0 (0)	3 (3)	9 (14)	38 (60)	32 (52)	12 (20)	7 (11)	2 (3)	0 (0)
NOT for school work:														
Average week day	6 (7)	30 (34)	34 (40)	14 (16)	7 (8)	4 (5)	5 (6)	12 (19)	32 (51)	28 (44)	19 (30)	6 (10)	1 (2)	2 (4)
Average weekend day	5 (6)	19 (22)	21 (24)	23 (27)	11 (13)	3 (4)	17 (20)	12 (20)	21 (34)	24 (38)	19 (31)	13 (21)	6 (10)	4 (7)

Figure 21. Frequency of students' Internet use by gender





Location of Internet use

Students were asked to report where they usually use the Internet and were provided with a list of responses from which to choose (Table 59). Students could choose more than one response to this question. The majority of students reported they usually used the Internet at home (Boys: 91%, *n* = 107; Girls: 94%, *n* = 153) or at school (Boys: 44%, *n* = 52; Girls: 55%, *n* = 89), while fewer students reported using the Internet at a friends' house (Boys: 29%, *n* = 34; Girls: 23%, *n* = 38), at the library (Boys: 19%, *n* = 22; Girls: 13%, *n* = 22) or at other places (e.g. another family member's house, their parents work or on a mobile phone) (Boys: 8%, *n* = 10; Girls: 7%, *n* = 12).

Table 59. Location of Internet use by gender

	Boys % (*n*)	**Girls** % (*n*)
I do not use the Internet	2 (2)	1 (1)
At home	91 (107)	94 (153)
At school	44 (52)	55 (89)
At a friends' house	29 (34)	23 (38)
At the library	19 (22)	13 (22)
Other	8 (10)	7 (12)

NB: Students could select more than one response

Students were then asked where at home they usually use the Internet (Table 60). Again, students could choose more than one response to this question. Half of students reported using the Internet at home in an open area (Boys: 46%, *n* = 54; Girls: 56%, *n* = 91), with a similar number of students reporting they usually used the Internet in the study or a separate room at home (Boys: 54%, *n* = 63; Girls: 56%, *n* = 91). Approximately one-quarter of students reported they usually used the Internet in their bedroom (Boys: 29%, *n* = 34; Girls: 26%, *n* = 42).

Table 60. Location of Internet use at home by gender

	Boys % (*n*)	**Girls** % (*n*)
I do not use the Internet at home	5 (6)	2 (4)
In an open area (e.g. lounge room, kitchen)	46 (54)	56 (91)
In my bedroom	29 (34)	26 (42)
In the study or separate room	54 (63)	56 (91)
In the bathroom	2 (2)	0 (0)
Other	8 (9)	2 (4)

NB: Students could select more than one response

Social networking site use

Approximately two-thirds of boys (63%, *n* = 73) and over three-quarters of girls (77%, *n* = 126) reported they use a social networking site (e.g., Facebook, MySpace, Club Penguin) or Instant Messenger (e.g., MSN) (Table 61). For boys, the most commonly used site was MSN (44%, *n* = 52), followed closely by Facebook (42%, *n* = 49) and Club Penguin (23%, *n* = 27) (Table 61). MSN was also the most popular site for girls (48%, *n* = 78), followed by Facebook (35%, *n* = 58), then Club Penguin (33%, *n* = 54).

Table 61. Type of social networking site or Instant Messenger used by gender

	Boys % (*n*)	Girls % (*n*)
I do not use this	30 (35)	21 (34)
Club Penguin	23 (27)	33 (54)
Bebo	5 (6)	1 (1)
MySpace	10 (12)	5 (8)
Facebook	42 (49)	35 (58)
MSN	44 (52)	48 (78)
Twitter	4 (5)	3 (5)
Other	16 (19)	19 (31)

NB: Students could select more than one response

Students were asked about the frequency with which they use a social networking site (SNS) or instant messenger (IM) site on an average day at school, before or after school and on the weekend (Table 62, Figure 22). Perhaps due to restricted access to these sites during school hours, more students reported they 'did not have this' to the question about frequency of use of SNS or IM on an average day at school (Boys: 66%, *n* = 73; Girls: 61%, *n* = 96), compared to the previous question about individual site usage (Boys: 30%, *n* = 35; Girls: 21%, *n* = 34). Of those who do use these sites at school, most students reported they used the site for less than half an hour on an **average day at school** (Boys: 26%, *n* = 29; Girls: 29%, *n* = 46). Most students who use a SNS or IM also reported using this for less than half an hour on an **average day before or after school** (Boys: 35%, *n* = 39; Girls: 31%, *n* = 50). Use of SNS and IM is more varied on an **average weekend day**. While less than one-quarter of students (Boys: 25%, *n* = 28; Girls: 14%, *n* = 23) reported they used these sites for less than half an hour on an average day of the weekend, a further one-fifth (Boys: 15%, *n* = 17; Girls: 22%, *n* = 36) reported using these sites for about one hour, and a similar proportion of students used the sites for about half an hour (Boys: 8%, *n* = 9; Girls: 17%, *n* = 27) and about two hours (Boys: 9%, *n* = 11; Girls: 12%, *n* = 20).

Students were asked a series of questions about actions they had taken in relation to their SNS and Internet use (Table 63, Figure 23). At pre-test, the majority of students reported they do not have online friends whom they have not met in person (Boys: 62%, *n* = 71; Girls: 60%, *n* = 96), they have set their SNS profile to private (Boys: 45%, *n* = 50; Girls:

55%, *n* = 87), they have not shared their password with others (Boys: 67%, *n* = 76; Girls: 66%, *n* = 105). Interestingly, about half of students reported that they have blocked or deleted someone who said something they think is rude or mean (Boys: 41%, *n* = 46; Girls: 54%, *n* = 86). Furthermore, about two-fifths of students reported they have not shared personal details with others (Boys: 38%, *n* = 43; Girls: 44%, *n* = 70) and about half have let their parents know who is on their friends list (Boys: 49%, *n* = 55; Girls: 53%, *n* = 83).

Post-test results

At post-test, the proportion of students who reported each of these actions was similar to pre-test results (Table 63). In general, while the proportion of boys who reported each action decreased overall, for most actions, the proportion of girls reporting they had undertaken this behaviour was stable. In particular, fewer boys reported having shared their password with others (10% at pre-test versus 4% at post-test), and having blocked or deleted someone who said something rude or mean (41% at pre-test versus 48% at post-test). The proportion of boys who reported they have not shared their personal details with anyone was stable (38% at pre-test versus 39% at post-test). At post-test, more girls reported they had not shared personal details with anyone (44% at pre-test versus 52% at post-test). The proportion of girls who reported they only have online friends they have met in person (60% at pre-test versus 66% at post-test), they have set their profile to private (55% at pre-test and 59% at post-test) and they have not shared their password with others (66% at pre-test versus 72% at post-test) was stable.

Table 62. Frequency of students' social networking or instant messenger site use by gender

	Boys % (*n*)							Girls % (*n*)						
	Don't have this	Less than half an hour	About half hour	About 1 hours	About 2 hours	About 3 hours	4 hours or more	Don't have this	Less than half an hour	About half hour	About 1 hours	About 2 hours	About 3 hours	4 hours or more
Average school day	66 (73)	26 (29)	5 (6)	1 (1)	0 (0)	1 (1)	0 (0)	61 (96)	29 (46)	5 (8)	3 (5)	1 (1)	0 (0)	0 (0)
Average day before or after school	38 (43)	35 (39)	12 (13)	8 (9)	6 (7)	0 (0)	1 (1)	31 (49)	31 (50)	18 (28)	11 (17)	6 (10)	2 (3)	1 (2)
Average weekend day	33 (38)	25 (28)	8 (9)	15 (17)	9 (11)	10 (11)	1 (1)	23 (38)	14 (23)	17 (27)	22 (36)	12 (20)	6 (9)	6 (9)

Figure 22. Frequency of students' social networking or instant messenger site use by gender

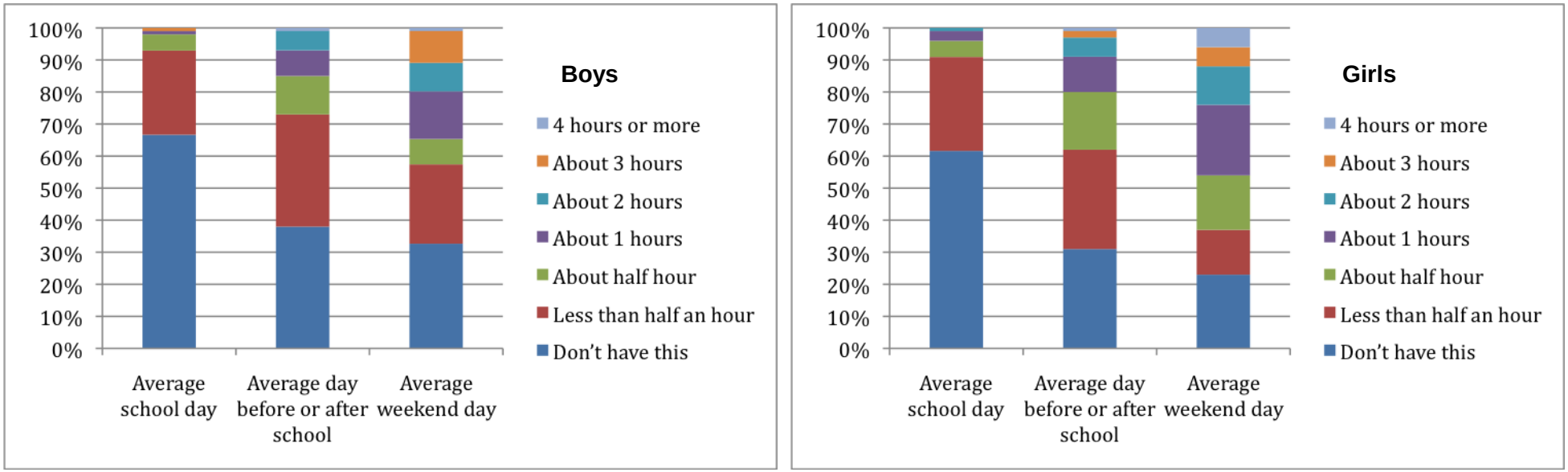
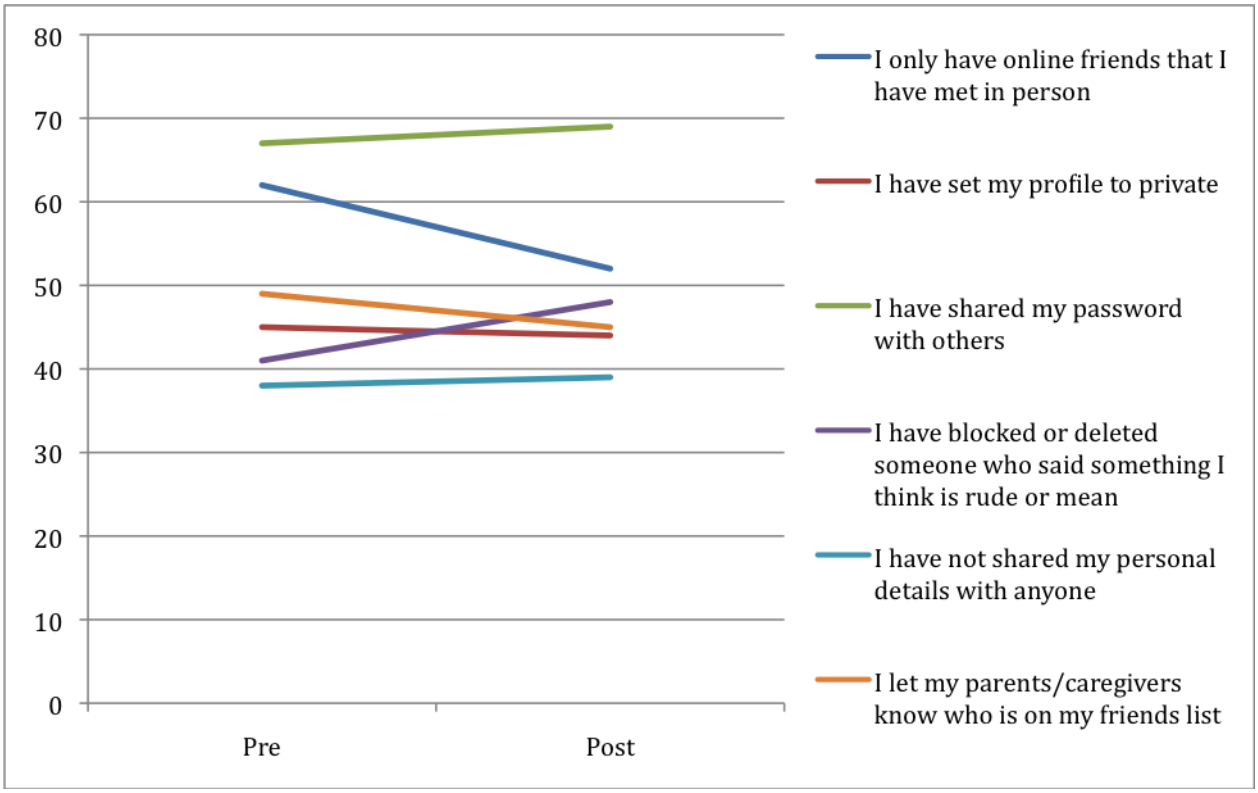


Table 63. Actions taken on social networking or instant messenger site by gender

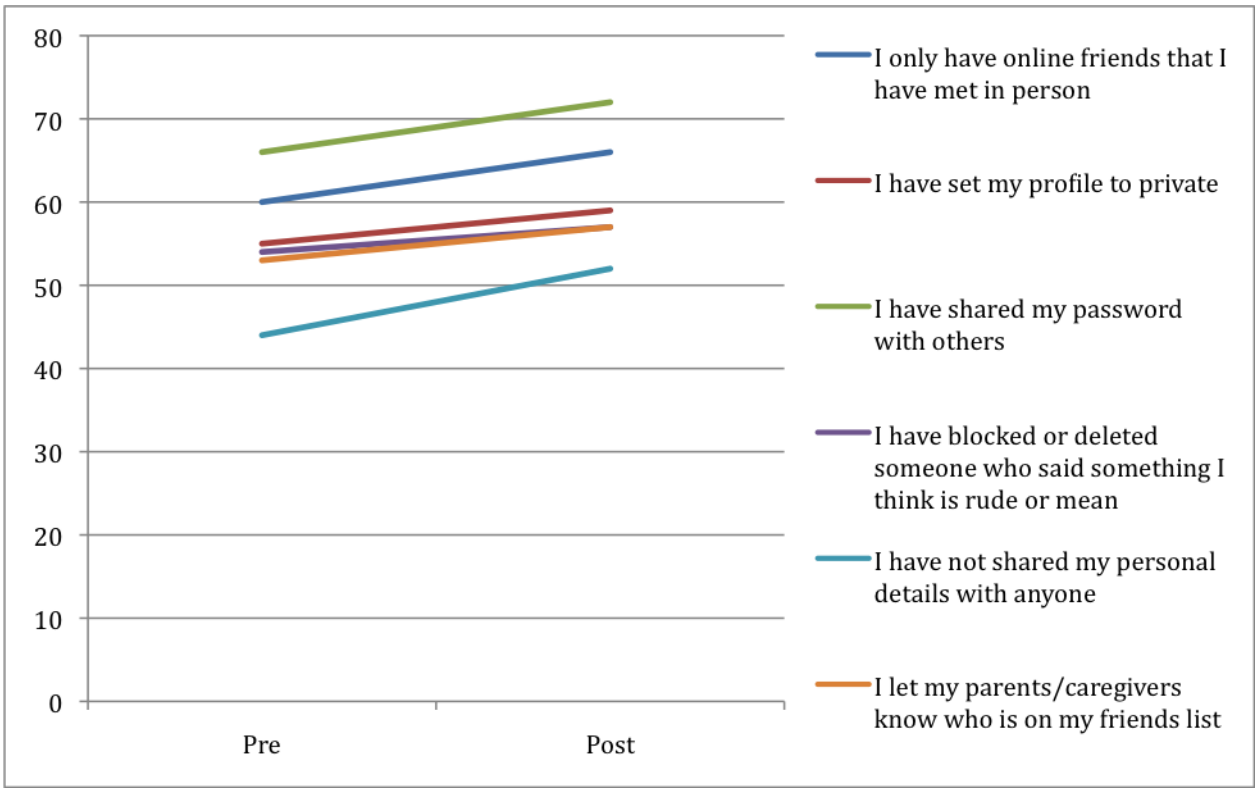
	Pre-test						Post-test					
	Boys % (*n*)			Girls % (*n*)			Boys % (*n*)			Girls % (*n*)		
	Yes	**No**	**Don't use**	**Yes**	**No**	**Don't use**	**Yes**	**No**	**Don't use**	**Yes**	**No**	**Don't use**
I only have online friends that I have met in person	62 (71)	13 (15)	25 (28)	60 (96)	19 (30)	22 (35)	52 (58)	20 (22)	28 (31)	66 (97)	13 (19)	21 (31)
I have set my profile to private	45 (50)	29 (32)	25 (28)	55 (87)	19 (30)	25 (40)	44 (48)	24 (27)	32 (35)	59 (87)	16 (23)	25 (37)
I have shared my password with others	10 (11)	67 (76)	23 (26)	13 (21)	66 (105)	21 (33)	4 (5)	69 (76)	27 (30)	9 (13)	72 (106)	19 (28)
I have blocked or deleted someone who said something I think is rude or mean	41 (46)	32 (36)	27 (31)	54 (86)	23 (37)	23 (36)	48 (53)	24 (26)	28 (31)	57 (83)	19 (28)	24 (35)
I have not shared my personal details with anyone	38 (43)	39 (44)	23 (26)	44 (70)	35 (56)	21 (33)	39 (43)	32 (35)	29 (32)	52 (77)	29 (42)	19 (28)
I let my parents/caregivers know who is on my friends list	49 (55)	26 (29)	26 (29)	53 (83)	25 (40)	22 (34)	45 (50)	25 (28)	29 (32)	57 (84)	22 (32)	21 (31)

Figure 23. Actions taken on social networking or instant messenger site by gender

Boys



Girls



When asked the highest number of friends or contacts they have on their SNS or IM (Table 64, Figure 24), approximately one-quarter of students reported they did not use these sites (Boys: 28%, *n* = 33; Girls: 24%, *n* = 39) and about one-quarter reported they had between zero and 19 friends/contacts (Boys: 25%, *n* = 29; Girls: 21%, *n* = 34). About one-quarter of girls (23%, *n* = 38) and 10% (*n* = 12) of boys had 20-49 friends while one-quarter of boys (20%, *n* = 23) and 15% (*n* = 25) of girls reported having 50-99 friends. Students were then asked what proportion of their friends/contacts list were known to them offline (Table 65, Figure 25). Most students reported they know all (Boys: 38%, *n* = 44; Girls: 39%, *n* = 64) or nearly all (Boys: 21%, *n* = 24; Girls: 22, *n* = 36) of their friends/contacts offline. Of those who report having a SNS or IM (*n* = 212), this equates to 51% who know all their online friends offline and a further 28% who know nearly all their online contacts offline.

Table 64. Number of friends on social networking and instant messaging sites by gender

	Boys		Girls	
	%	*n*	%	*n*
I do not have any of these accounts	28	33	24	39
0-19	25	29	21	34
20-49	10	12	23	38
50-99	20	23	15	25
100-149	7	8	9	14
150-199	4	5	2	4
200-299	3	3	5	8
300 or more	3	3	1	1

Figure 24. Number of friends on social networking and instant messaging sites by gender

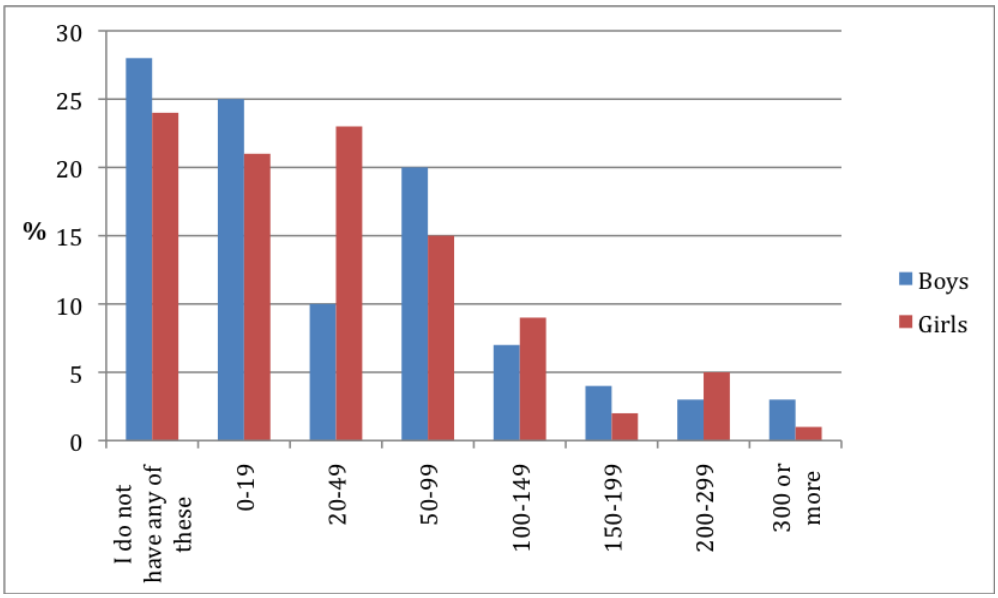
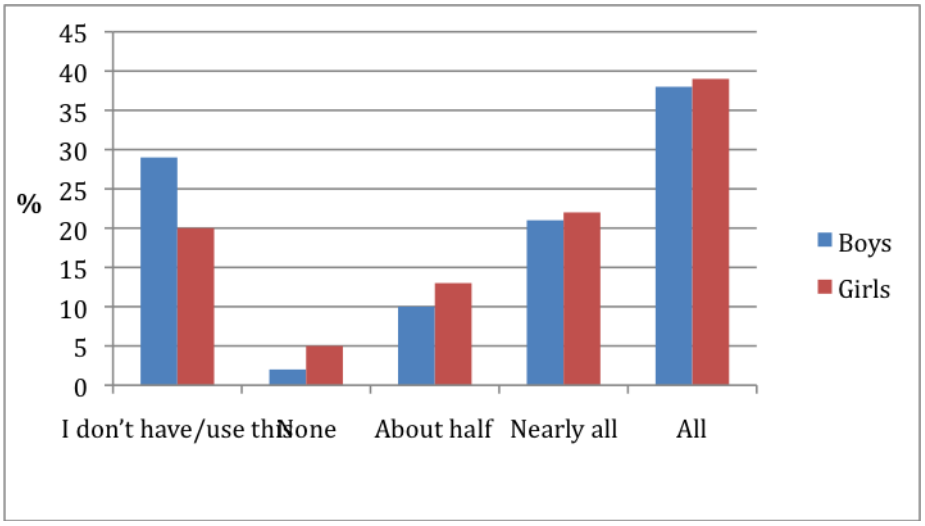


Table 65. Proportion of online friends known offline by gender

	Boys		Girls	
	%	n	%	n
I don't have/use this	29	34	20	33
None	2	2	5	8
About half	10	12	13	22
Nearly all	21	24	22	36
All	38	44	39	64

Figure 25. Proportion of online friends known offline by gender



Chat site use

Students were asked to list up to three chat sites they used on the Internet. Fewer girls (30%, *n* = 48) than boys (39%, *n* = 45) reported they do not use chat sites on the Internet.

Online game use

The majority of students reported they play games on the Internet (e.g., World of Warcraft) (Boys: 85%, *n* = 97; Girls: 74%, *n* = 116). Amongst these students, the most popular mode of online game playing was via a computer (Boys: 75%, *n* = 88; Girls: 70%, *n* = 114), with much smaller numbers of students reporting using other consoles for example, Nintendo DSi (Boys: 21%, *n* = 25; Girls: 31%, *n* = 51), PlayStation including PS2 and PS3 (Boys: 32%, *n* = 37; Girls: 12%, *n* = 20) and Xbox (Boys: 25%, *n* = 29; Girls: 5%, *n* = 9) (Table 66).

Table 66. Online game use by gender

	Boys		Girls	
	%	*n*	%	*n*
I do not play online games	9	11	18	30
Nintendo DSi / DS / DS Lite	21	25	31	51
PlayStation Portable (PSP)	18	21	2	4
PlayStation (e.g. PS2, PS3)	32	37	12	20
Xbox	25	29	5	9
Computer	75	88	70	114
Other:	17	20	20	33
Wii	11	13	8	14
Mobile phone	1	1	2	3
iPod / iTouch	2	2	5	8

NB: Students could select more than one response

When playing online games, girls more than boys often play games that don't require interaction with others online (Boys: 16%, *n* = 17; Girls: 37%, *n* = 58) (Table 67). About one-quarter of students report playing online games with only people they have met in person (Boys: 25%, *n* = 27; Girls: 20%, *n* = 32) and one-half of boys and one-quarter of girls reported playing online games with both others whom they have and have not met in person (Boys: 48%, *n* = 52; Girls: 24%, *n* = 38).

Table 67. Online game contacts by gender

	Boys		Girls	
	%	*n*	%	*n*
ONLY people you have met in person	25	27	20	32
ONLY people you have never met	1	1	0	0
BOTH people you know in person and people you have never met	48	52	24	38
I don't play games online with any other person	16	17	37	58
I don't play online games	11	12	18	29

Contact with unknown other

Students were asked to report the frequency with which they have ever been contacted online by someone whom they have not met in person (Tables 68 and 69). The majority of students reported they either did not have a **SNS** (Boys: 33%, *n* = 36; Girls: 31%, *n* = 51) or that they had not been contacted by someone they have not met in person on this site (Boys: 33%, *n* = 36; Girls: 35%, *n* = 56). Smaller numbers of students reported some contact on their social networking site by someone they have not met, ranging from once (Boys: 8%, *n* = 9; Girls: 11%, *n* = 18) to more than five times (Boys: 9%, *n* = 10; Girls: 7%, *n* = 12). At post-test, the proportion of boys and girls who reported having been contacted on their social networking site by someone they have not met in person increased (at pre-test 34% of boys and 33% of girls had any contact versus 38% of boys and 42% of girls at post-test).

Nearly half of boys (43%, *n* = 48) and one-third of girls (39%, *n* = 62) in this study did not use MSN; however, among those who do, most students (Boys: 33%, *n* = 37; Girls: 40%, *n* = 64) report never having received contact by someone they have not met in person. The

frequency of students' report of contact on MSN by someone they have not met in person displayed a generally negative trend (i.e., increasingly fewer students reported higher levels of contact with someone whom they had not met in person). At post-test, the frequency with which boys reported being contacted on MSN by someone they don't know more than five times rose to 7% (from 4% at pre-test). Moreover, the frequency with which girls reported being contacted on MSN only once increased from 8% to 12% and contact two to three times rose from 4% at pre-test to 12% at post-test.

Almost all students reported they either did not use a **webcam** (Boys: 53%, *n* = 59; Girls: 51%, *n* = 81) or that they had never been contacted by someone they had not met in person on their webcam (Boys: 42%, *n* = 47; Girls: 45%, *n* = 71).

Over 80% of students reported they either did not have a **mobile phone** (Boys: 59%, *n* = 65; Girls: 43%, *n* = 68) or that they had never been contacted by someone they had not met in person on their mobile phone (Boys: 26%, *n* = 29; Girls: 37%, *n* = 59). Smaller numbers of students reported some contact: 4% (*n* = 5) of boys and 11% (*n* = 18) of girls reported being contacted once, 8% (*n* = 9) of boys and 5% (*n* = 8) of girls reported being contacted two to three times, 1% (*n* = 1) of boys and 2% (*n* = 3) of girls reported being contacted four to five times and 1% (*n* = 1) of boys and 2% (*n* = 3) of girls reported being contacted more than five times on their mobile phone by someone they have not met in person. The proportion of boys who reported being contacted four or five times on their mobile phone by someone they had not met rose from pre-test to post-test (1% to 3% respectively) and for more than five times this rose from 1% at pre-test to 4% at post-test.

At pre-test, most students had not used (Boys: 41%, *n* = 46; Girls: 44%, *n* = 69) nor been contacted (Boys: 32%, *n* = 36; Girls: 44%, *n* = 69) on a **chat site** by someone they had not met in person. At pre-test, 84% (*n* = 9) of boys and 4% (*n* = 7) of girls had been contacted by someone they did not know in person on a chat site once. For girls, this increased at post-test to 9% (*n* = 13).

The majority of students reported they either did not have/use a **blog** (Boys: 57%, *n* = 63; Girls: 61%, *n* = 97) or that they had never been contacted on their blog by someone they had not met in person (Boys: 35%, *n* = 39; Girls: 33%, *n* = 52).

While two-thirds of students reported they had never been contacted in an **online game** by someone they had not met in person (Boys: 33%, *n* = 36; Girls: 47%, *n* = 76) or they did not use/have online games (Boys: 26%, *n* = 26; Girls: 30%, *n* = 48), some students had experienced contact. For boys, report of contact five or more times rose from 23% (*n* = 25) at pre-test to 28% (*n* = 30) at post-test.

Students who said they had been contacted in other ways by someone they did not know in person most frequently cited this was through **email** (Boys: 1%, *n* = 1; Girls: 2%, *n* = 3).

Table 68. Frequency of contact by someone male student has not met in person

	Pre-test % (*n*)						Post-test % (*n*)					
	Don't have/use	**Never**	**Only 1 time**	**2-3 times**	**4-5 times**	**More than 5 times**	**Don't have/use**	**Never**	**Only 1 time**	**2-3 times**	**4-5 times**	**More than 5 times**
Social networking site	33 (36)	33 (36)	8 (9)	14 (16)	3 (3)	9 (10)	37 (41)	24 (27)	8 (9)	16 (18)	2 (2)	12 (13)
Instant messenger	43 (48)	33 (37)	8 (9)	9 (10)	3 (3)	4 (4)	40 (43)	32 (34)	7 (8)	10 (11)	3 (3)	7 (8)
Webcam	53 (59)	42 (47)	2 (2)	0 (0)	0 (0)	3 (3)	55 (61)	35 (39)	3 (3)	1 (1)	4 (4)	2 (2)
Mobile phone	59 (65)	26 (29)	4 (5)	8 (9)	1 (1)	1 (1)	55 (61)	26 (29)	6 (7)	5 (6)	3 (3)	4 (4)
Chat room	41 (46)	32 (36)	8 (9)	6 (7)	2 (2)	10 (11)	44 (48)	30 (33)	6 (7)	6 (7)	3 (3)	11 (12)
Blog	57 (63)	35 (39)	4 (4)	3 (3)	0 (0)	2 (2)	55 (60)	33 (36)	2 (2)	5 (6)	1 (1)	4 (4)
Online game	24 (26)	33 (36)	6 (7)	5 (6)	8 (9)	23 (25)	28 (30)	29 (31)	6 (7)	6 (7)	3 (3)	28 (30)
Other	--	--	0 (0)	2 (2)	1 (1)	0 (0)	--	--	2 (2)	0 (0)	0 (0)	2 (2)

Table 69. Frequency of contact by someone female student has not met in person

	Pre-test % (*n*)						Post-test % (*n*)					
	Don't have/use	**Never**	**Only 1 time**	**2-3 times**	**4-5 times**	**More than 5 times**	**Don't have/use**	**Never**	**Only 1 time**	**2-3 times**	**4-5 times**	**More than 5 times**
Social networking site	31 (51)	35 (56)	11 (18)	12 (19)	3 (5)	7 (12)	26 (38)	31 (46)	11 (16)	21 (31)	3 (5)	7 (10)
Instant messenger	39 (62)	40 (64)	8 (13)	4 (6)	6 (10)	3 (5)	38 (55)	32 (46)	12 (18)	12 (17)	2 (3)	3 (5)
Webcam	51 (81)	45 (71)	1 (2)	1 (2)	1 (2)	1 (1)	53 (77)	40 (58)	3 (5)	3 (5)	0 (0)	0 (0)
Mobile phone	43 (68)	37 (59)	11 (18)	5 (8)	2 (3)	2 (3)	45 (65)	34 (50)	12 (17)	4 (6)	2 (3)	3 (4)
Chat room	44 (69)	44 (69)	4 (7)	3 (5)	1 (1)	4 (6)	46 (67)	34 (50)	9 (13)	5 (8)	1 (2)	4 (6)
Blog	61 (97)	33 (52)	5 (8)	1 (1)	0 (0)	1 (1)	61 (88)	33 (48)	1 (2)	2 (3)	1 (2)	1 (1)
Online game	30 (48)	47 (76)	10 (16)	6 (9)	1 (2)	6 (9)	29 (42)	43 (63)	13 (19)	8 (11)	3 (4)	4 (6)
Other	--	--	1 (2)	1 (1)	0 (0)	1 (1)	--	--	2 (3)	1 (2)	0 (0)	1 (1)

Finally, students were asked what action they would take if they were (hypothetically) contacted online by someone they did not know (Table 70, Figure 26). At pre-test, the majority of students reported that should this occur, they would not respond to the messages (Boys: 66%, *n* = 77; Girls: 80%, *n* = 131), leave the chat session or log out immediately (Boys: 61%, *n* = 71; Girls: 79%, *n* = 128), block the person who contacted them (Boys: 70%, *n* = 82; Girls: 83%, *n* = 136), keep the messages as evidence (Boys: 51%, *n* = 60; Girls: 55%, *n* = 90), talk to a parent about it (Boys: 62%, *n* = 73; Girls: 76, *n* = 124), talk to a friend about it (Boys: 57%, *n* = 67; Girls: 69%, *n* = 112), talk to other family members about it (Boys: 55%, *n* = 64; Girls: 56%, *n* = 91), set their social networking site profile to private (Boys: 62%, *n* = 72; Girls: 80%, *n* = 131) and not open the messages or emails sent to them from the person they did not know in person (Boys: 65%, *n* = 76; Girls: 79%, *n* = 129). Fewer students reported they would talk to a teacher/principal (Boys: 34%, *n* = 40; Girls: 32%, *n* = 53), talk to the police (Boys: 25%, *n* = 29; Girls: 18%, *n* = 29), or talk to their Internet Service Provider (Boys: 13%, *n* = 15; Girls: 19%, *n* = 31) about the contact.

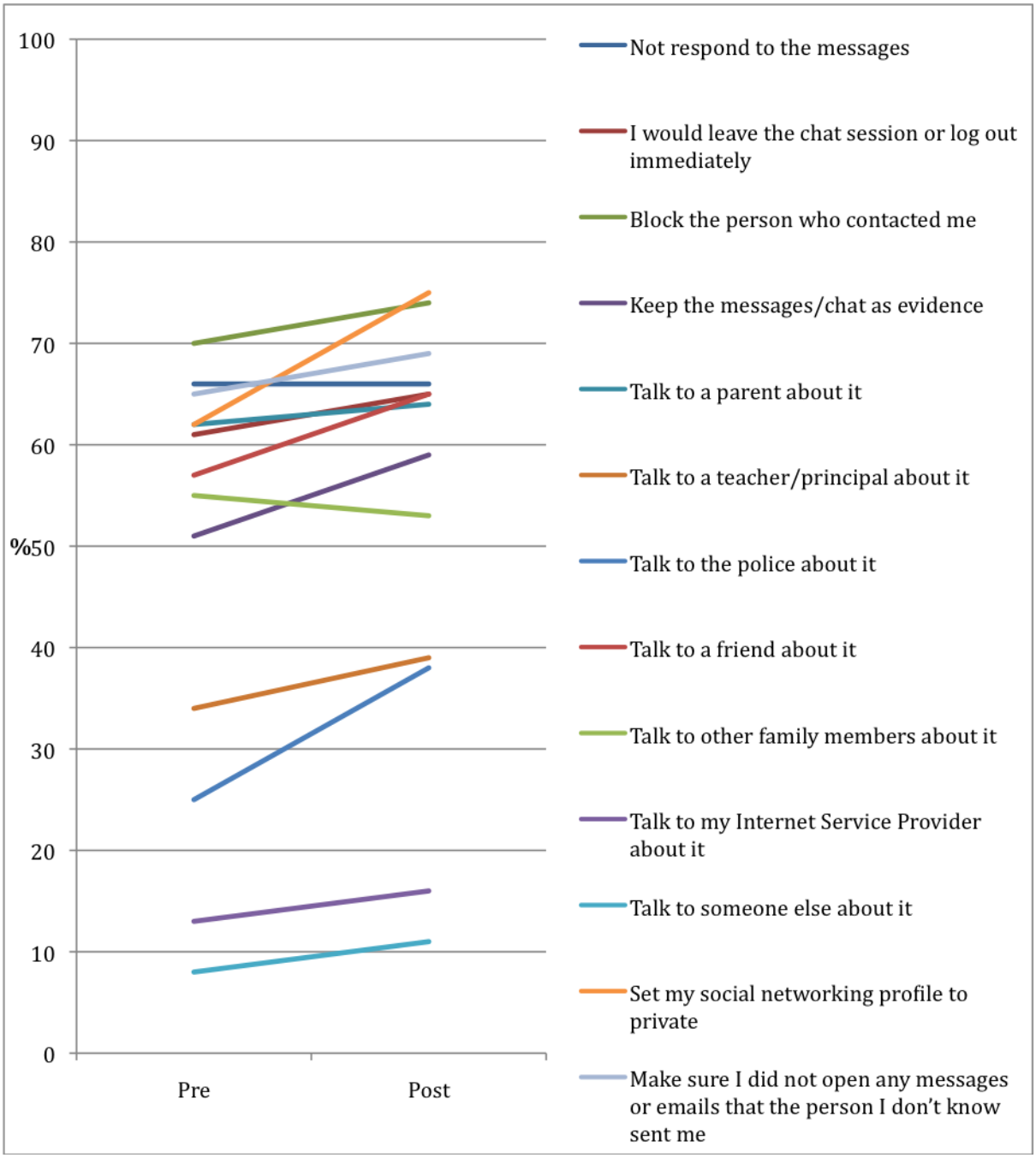
At post-test, the proportion of boys who reported they would talk to the police if contacted online by someone they did not know (38%, *n* = 43) increased from post-test (25%, *n* = 29). This was also true for girls who rose from 18% (*n* = 29) at pre-test to 24% (*n* = 38) at post-test. The proportion of boys who reported they could talk to a friend if contacted online by someone they did not know increased from pre-test (62%, *n* = 72) to post-test (75%, *n* = 85), although this was not true for girls (Pre-test: 80%, *n* = 131; Post-test: 77%, *n* = 123).

Table 70. Likely response if contacted online by someone unknown by gender

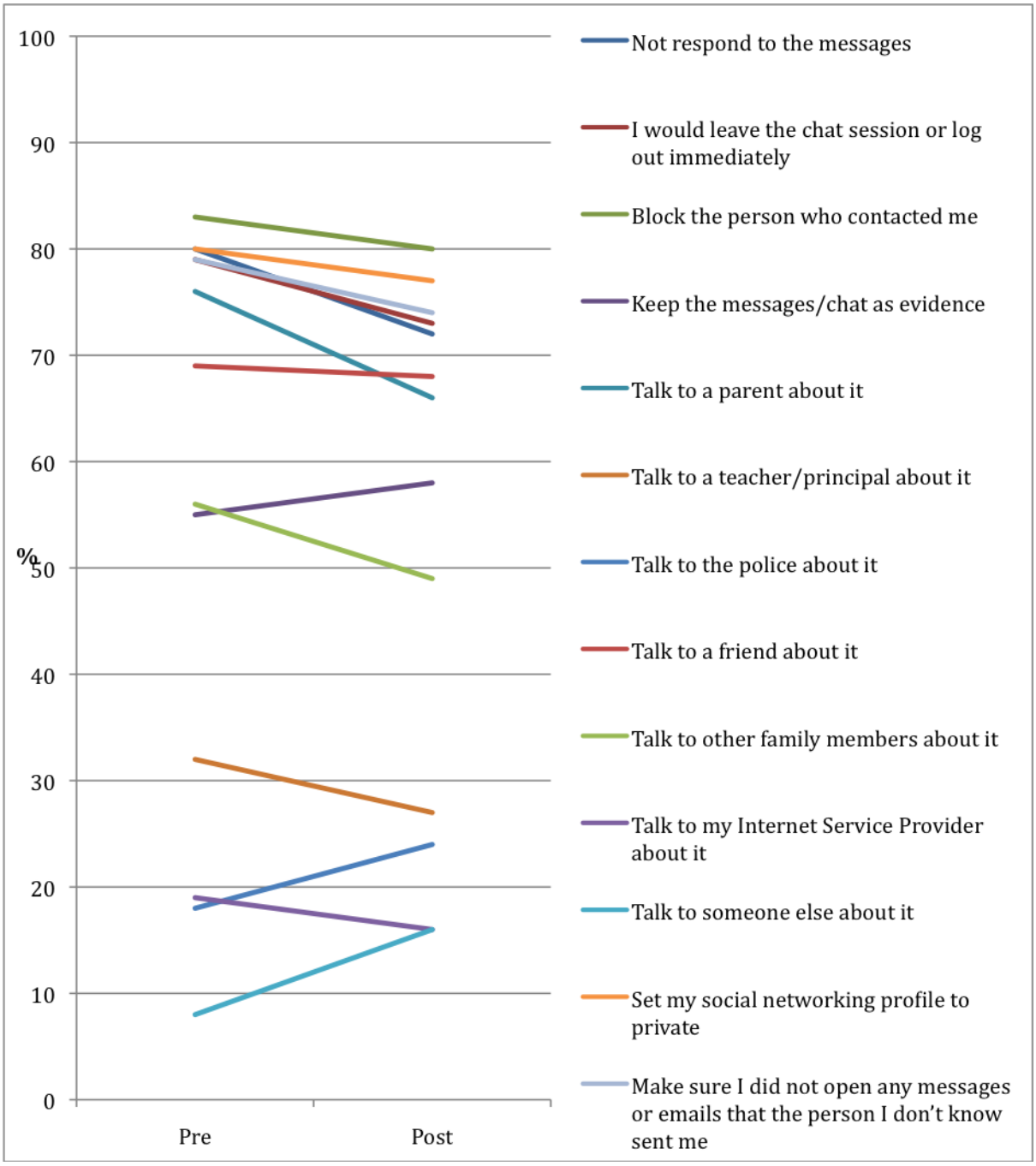
	Pre-test % (*n*)				Post-test % (*n*)			
	Boys		Girls		Boys		Girls	
	No	Yes	No	Yes	No	Yes	No	Yes
Not respond to the messages	34 (40)	66 (77)	20 (32)	80 (131)	34 (39)	66 (75)	28 (45)	72 (115)
I would leave the chat session or log out immediately	39 (46)	61 (71)	21 (35)	79 (128)	35 (40)	65 (74)	27 (44)	73 (116)
Block the person who contacted me	30 (35)	70 (82)	17 (27)	83 (136)	26 (30)	74 (84)	20 (32)	80 (128)
Keep the messages/chat as evidence	49 (57)	51 (60)	45 (73)	55 (90)	41 (47)	59 (67)	42 (68)	58 (92)
Talk to a parent about it	38 (44)	62 (73)	24 (39)	76 (124)	36 (41)	64 (73)	34 (54)	66 (106)
Talk to a teacher/principal about it	66 (77)	34 (40)	68 (110)	32 (53)	61 (70)	39 (44)	73 (116)	27 (44)
Talk to the police about it	75 (88)	25 (29)	82 (134)	18 (29)	62 (71)	38 (43)	76 (122)	24 (38)
Talk to a friend about it	43 (50)	57 (67)	31 (51)	69 (112)	35 (40)	65 (74)	32 (52)	68 (108)
Talk to other family members about it	45 (53)	55 (64)	44 (72)	56 (91)	47 (54)	53 (60)	51 (81)	49 (79)
Talk to my Internet Service Provider about it	87 (102)	13 (15)	81 (132)	19 (31)	84 (96)	16 (18)	84 (135)	16 (25)
Talk to someone else about it	92 (108)	8 (9)	92 (150)	8 (13)	89 (101)	11 (13)	84 (135)	16 (26)
Set my social networking profile to private	38 (45)	62 (72)	20 (32)	80 (131)	25 (29)	75 (85)	23 (37)	77 (123)
Make sure I did not open any messages or emails that the person I don't know sent me	35 (41)	65 (76)	21 (34)	79 (129)	31 (35)	69 (79)	26 (41)	74 (119)
Other	--	3 (3)	--	4 (7)	--	3 (4)	--	3 (5)

Figure 26. Likely response if contacted online by someone unknown by gender

Boys



Girls


100
90
80
70
60
%
50
40
30
20
10
0
Pre
Post
Not respond to the messages
I would leave the chat session or log out immediately
Block the person who contacted me
Keep the messages/chat as evidence
Talk to a parent about it
Talk to a teacher/principal about it
Talk to the police about it
Talk to a friend about it
Talk to other family members about it
Talk to my Internet Service Provider about it
Talk to someone else about it
Set my social networking profile to private
Make sure I did not open any messages or emails that the person I don't know sent me

Participants' responses to the above question were summed to create a score of positive actions students would take if they were contacted online by someone they did not know in person (Table 71). Scores ranged from zero to 13. At pre-test, 47% (*n* = 55) of boys and 54% (*n* = 88) of girls reported they would do enough actions that classified them as being in the 'average or above category'. The proportion of students classified as this at post-test was similar (Boys: 46%, *n* = 53; Girls: 51%, *n* = 82). While the actual number of students who reported this decreased, this may be due to student absenteeism on the post-test data collection date.

Table 71. Score of positive actions students would undertake if contacted by someone they did not know in person by gender

	Pre-test				Post-test			
	Boys		Girls		Boys		Girls	
	%	*n*	%	*n*	%	*n*	%	*n*
Lower than average	53	62	46	75	54	61	49	78
Average or above	47	55	54	88	46	53	51	82

Table 72 displays the same results of 'positive action score' with students separated into three categories. The mean positive action score at pre-test was 6.91 with a standard deviation of 3.22. Hence, students with a positive action score lower than one standard deviation below the mean were classified as 'low identifiers' (i.e. they were able to identify four or fewer strategies to undertake if contacted online by someone unknown to them) and students with a positive action score equal to or greater than one standard deviation above the mean were classified as 'high identifiers'. Students who scored between five and nine on the positive action score were classified as 'moderate identifiers'. As shown in Table 72, the majority of students could be classified as moderate identifiers.

Table 72. Three-category score of positive actions students would undertake if contacted by someone they did not know in person by gender

	Pre-test				Post-test			
	Boys		Girls		Boys		Girls	
	%	*n*	%	*n*	%	*n*	%	*n*
Low identifiers	31	36	15	24	25	28	19	31
Moderate identifiers	50	59	66	107	51	58	58	93
High identifiers	19	22	20	32	25	28	23	36

Paired (or dependent) t-tests were conducted to determine any significant changes in the number of positive actions students reported they would take if they were contacted online by someone they did not know in person. These data were compared to identify changes in proposed behaviours amongst boys and girls individually. These analyses demonstrate:

- At pre-test, more girls than boys were scored 'average or above' in terms of the number of actions they identified were things they would do if contacted online by someone they did not know (54% and 46% respectively).
- At post-test, this trend was repeated (score average or above: Girls 51%; Boys 45%).
- In general, boys reported significantly more actions at post-test (M = 7.1, SE = 0.3) than at pre-test (M = 6.1, SE = 0.34), t(112) = -2.530, p = 0.013.
- In general, there was no statistically significant difference between the pre-test and post-test scores of girls (p = 0.148).

This suggests the CSD activity may be particularly useful for boys by increasing their average awareness of actions to take (e.g., telling parents, teachers, friends) if contacted online by someone they do not know in person.

CSD activity recall

In the post-test questionnaire, students were asked a series of questions to measure how well they recalled various components of the CSD activity. This section presents the results of the eight questions relating to students' recollection of the game (Table 73). It is important to note that these items were presented in a multiple-choice format. First, students were asked to recall the age of the girl (Sarah) in the story. Almost half of boys recalled the age of the girl in the story correctly, being 13 years (44%, *n* = 48), while 43% (*n* = 62) of girls could correctly recall this fact. Students were next asked to recall who had been contacting Sarah. Almost all students answered this question correctly with the response 'Kel17' (Boys: 94%, *n* = 104; Girls: 95%, *n* = 140). The majority of students were able to recall Sarah's hobby as rollerblading (Boys: 88%, *n* = 97; Girls: 89%, *n* = 130).

The majority of students recalled that the boy got Sarah's mobile number online (Boys: 82%, *n* = 91; Girls: 80%, *n* = 117). In the story, the boy wanted to take Sarah to the skate park. Almost all students answered this question correctly (Boys: 85%, *n* = 93; Girls: 93%, *n* = 136). Students were able to recall the location of Sarah's computer at home quite well with 82% (*n* = 91) of boys and 88% (*n* = 130) of girls reporting the computer was located in her bedroom. Towards the end of the scenario, students found out the person waiting to meet Sarah was 37 years old. More girls (73%, *n* = 107) than boys (54%, *n* = 60) answered this question correctly. Finally, students were asked to recall whether police were called in the story. While 17% (*n* = 19) of boys and 10% (*n* = 14) of girls could not remember if this occurred, 69% (*n* = 77) and 83% (*n* = 121) of boys and girls (respectively) answered correctly that the police had been called.

Table 73. Students' recall of components of CSD script by gender

		Boys		Girls	
		%	*n*	%	*n*
Age of girl in story (Sarah)	I don't remember	26	29	26	38
	13 years	44	48	43	62
	14 years	13	14	19	28
	15 years	17	19	12	17
Person contacting Sarah	I don't remember	4	4	2	3
	Tel 15	0	0	1	2
	Kel17	94	104	95	140
	Tim16	3	3	1	2
Sarah's hobby	I don't remember	10	11	6	9
	Rollerblading	88	97	89	130
	Biking	2	2	3	5
	Running	0	0	1	2
How boy got Sarah's mobile phone number	I don't remember	12	13	10	14
	She gave it to him	6	7	10	14
	They had friends in common	0	0	1	1
	He got it online	82	91	80	117
Where the boy wanted to take Sarah	I don't remember	10	11	4	6
	His house	5	6	3	4
	Local skate park	85	93	93	136
	To the cinema	0	0	1	1
Location of Sarah's home computer	I don't remember	15	16	9	14
	In her bedroom	82	91	88	130
	In the family room	2	2	1	2
	She does not have one at home	2	2	1	1
Age of person waiting to meet Sarah	I don't remember	17	19	8	12
	17 years	18	20	13	19
	37 years	54	60	73	107
	21 years	11	12	6	9
Police contacted in story	I don't remember	17	19	10	14
	Yes	69	77	83	121
	No	13	15	7	11

Appendix 9. References

1. NetSmartz. http://www.netsmartz.org/Overview/AboutUs. 2011.
2. Chibnall, S., et al., *I-safe evaluation. Final Report*, F. Caliber Association, Editor. 2006.
3. Crombie, G., & Trinneer, A., *Children and Internet Safety: An evaluation of the Missing Program*, R.a.E. Section, Editor. 2003.
4. Wishart, J.M., Oades, C. E., & Morris, M., *Using online role play to teacher Internet safety awareness.* Computers & Education, 2007. **48**: p. 460-473.
5. Dooley, J.J., et al., *Review of existing Australian and international cyber-safety research*. 2009, Child Health Promotion Research Centre, Edith Cowan University: Perth.
6. Dede, C., *Planning for neomillennial learning styles.* Educause, 2005. **28**(11).
7. Oblinger, D.G. and J.L. Oblinger, *Educating the net generation*. 2005, Educause.
8. Prensky, M., *Digital natives, digital immigrants, Part II: do they really think differently?* On the Horizon, 2001. **9**(6): p. 1-9.
9. Mumtaz, S., *Children's enjoyment and perception of computer use in the home and the school.* Computers and Education, 2001. **36**(4): p. 347-362.
10. Gee, J.P., *Good video games and good learning: collected essays on video games, learning and literacy*. 2007, New York: Peter Lang Publishing, Inc.
11. Papert, S., *Mindstorms: children, computerns and powerful ideas*. 1980, New York: Basic Books.
12. Rieber, L.P., *Seriously considering play: designing interactive learning environments based on the blending of microworlds, simulations, and games.* Educational Technology Research and Development, 1996. **44**(2): p. 43-58.
13. Balasubranmanian, N. and B. Wilson, *Games and simulations*. n.d.
14. Lepper, M. and T. Malone, *Intrinsic motivation and instrucional effectiveness in computer-based education*, in *Aptitudes, learning and instruction, II: cognative, and affective process analysis*, R.E. En Snow and M.J. Farr, Editors. 1987, Lawrence Earlbaum Association: Hollsdale, NJ.
15. Shih, J., et al., *The influence of collaboration styles to children's cognitive performance in digital problem-solving game "William Adventure": a comparative study.* Computers & Education, 2010: p. 1-12.
16. McGonigal, J. *This is not a game: Immersive aesthetics and collective play*. in *Digital Arts and Culture*. 2003. Melbourne, Australia: Royal Melbourne Institute of Technology.
17. Iqbalm, A., M. Kankaanrants, and P. Neittaanmaki, *Engaging learners through virtual worlds.* Procedia Social and Behavioural Sciences, 2010. **2**: p. 3198-3205.
18. Vanlanduyt, L. and I. De Cleyn, *Internet parenting styles and the impact on Internet use of primary school children.* Computers and Education, 2010. **55**: p. 454-464.
19. Vanlanduyt, L. and I. De Cleyn, *Invloed van Internet bij jongeren: een uitdaging op school en thuis.* 2007.
20. Squire, K., *Video games in education.* Internatioanl Journal of Intelligent Simulations and Gaming, 2003. **2**(1).

21. McFarlane, A., A. PSparrowhawk, and Y. Heald, *Report on the educational use of games: an exploration by Teem of the contribution which games can make to the education process*. 2002.

22. Funk, J.B., *Electronic Games*, in *Children, adolescents and the media*, V.C. Strasburger and B.J. Wilson, Editors. 2002, Sage Publications: Thousand Oaks, CA. p. 117-144.

23. Gross, M., *Advergames and the effects of game-product congruity. .* Computers in Human Behaviour, 2010.

24. Kim, M.G. and J. Kim, *Cross validation of reliability, convergent and discriminant validity for the problematic online game use scale.* Computers in Human Behaviour, 2010. **26**: p. 389-398.

25. Peng, W., *Design and evaluation of a computer game to promote a healthy diet for young adults.* Health Communication, 2009. **24**: p. 115-127.

26. Annetta, L., et al., *Investigating the impact of video games on high school students' engagement and learning about genetics.* Computers and Education, 2009. **53**: p. 74-85.

27. Durken, K. and B. Barber, *Not so doomed: computer game play and positive adolescent development.* Journal of Applied Developmental Psychology, 2002. **23**(4): p. 373-392.

28. Malone, F., *Toward a theory of intrinsically motivation instruction.* Cognitive Science, 1980. **5**(4): p. 333-369.

29. Papastergiou, M., *Digital game-based learning in high school computer science education: impact on educational effectiveness and student motivation.* Computers and Education, 2009. **52**(1): p. 1-12.

30. Chapman, D., *Video games in the classroom*. 2004, Wisconsin Technology Network.

31. Green, S. and D. Bavelier, *Action video game modifies visual selective attention.* Nature, 2003. **423**: p. 534-537

32. Ahlfeldt, S., S. Mehta, and T. Sellnow, *Measurement and analysis of student engagement in university classess where varying levels of PBL methods of instruction are in use.* Higher Education Research and Development, 2005. **24**(1): p. 5-20.

33. Taradi, S.K., et al., *Blending problem-based learning with Web technology positively impacts student learningoutcomes in acid-base physiology.* Journal of Advanced Psychological Education, 2005. **29**: p. 35-39.

34. Barab, S., et al., *Making learning fun: Quest Atlantis, a game without guns.* Educational Technology Research and Development, 2005. **53**(1): p. 86-107.

35. Lee, K.M. and W. Peng, *A brief biography of computer game studies*, in *Playing computer games: motives, responses and consequences*, P. Vorderer and J. Bryant, Editors. 2006, Lawernce Erlbaum Associates, Inc.: Mahwah, NJ. p. 325-345.

36. Lieberman, D.A., *What can we learn from playing interactive games?*, in *Playing computer games: motives, responses and consequences*, P. Vorderer and J. Bryant, Editors. 2006, Lawrence Relbaum Associates: Mahwah, NJ.

37. Green, H., et al., *Personalisation and Digital Technologies*. 2007, Bristol: Futurelab.

38. Clark, D. *Learning by playing: can computer games and simulations support teaching and learning for post-16 learners in formal, workplace and informal learning contexts*. in *Computer games in education and training* 2003. London.

39. Becta. *Computer Games in Education Project*. 2001.

40. Kirriemuir, J. and A. McFarlane. *Use of computer and video games in the classroom*. in *Digital Games Research Association, Level Up Conference*. 2003. Utrecht, Netherlands: University of Utrecht.

41. Rosas, R., et al., *Beyond Nintendo: design and assessment of educational video games for first and second grade students. .* Computers and Education, 2003. **40**: p. 71-94.

42. Bennett, N., L. Wood, and S. Rogers, *Teaching Through Play: Teachers' Thinking and Classroom Practice* 1997, Buckingham: Open University Press.

43. Glanz, K., F. Lewis, and B. Rimer, *Health behaviour and health education*. 1997, California, USA Jossey-Bass Publishers.

44. Nutbeam, D. and E. Harris, *Theory in a nutshell. A guide to health promotion theory*. 1999: McGraw-Hill Education.

45. Rogers, R.W., *A protection motivation theory of fear appeals and attitude change.* Journal of Psychology 1975: p. 93-114.

46. Gingiss, P., C. Roberts-Gray, and M. Boerm, *Bridge-It: a system for predicting implementation fidelity for school-based tobacco prevention programs* Prevention Science, 2006. **7**: p. 197-207.

47. Rogers, E.M., *Diffusion of preventive innovations.* Addictive Behaviours, 2002. **27**: p. 989-993.

48. Booth, M.L. and O. Samdal, *Health-promoting schools in Australia: models and measurement. .* Australian and New Zealand Journal of Public Health, 1997. **21**(4): p. 365-370.

49. Allensworth, D. and L. Kolbe, *The comprehensive school health program: exploring an expanded concept.* Journal of School Health, 1987. **57**(10): p. 409-412.

50. Weigle, K.L., *Positive behaviour support as a model for promoting educational inclusion.* Journal of The Association for Persons with Severe Handicaps, 1997. **22**: p. 36-48.

51. Bandura, A., *Social learning theory*. 1977, Upper Saddle River, NJ: Prentice Hall.

52. Bourgonjon, J., et al., *Students' perceptions about the use of video games in the classroom.* Computers and Education, 2010. **54**: p. 1145-1156.

53. Derryberry, A., *Serious Games: online games for learning*. 2007.

54. Bandura, A., *Health promotion by social cognitive means.* Health Education and Behavior, 2004. **31**(2): p. 143-164.

55. Catford, J., *The Bangkok Conference: steering countries to build national capacity for health promotion.* Health Promotion International, 2005. **20**(1): p. 1-6.

56. Hawe, P., et al., *Indicators to help with capacity building in health promotion*. 1999, Australian Centre for Health Promotion: Sydney.

57. International Union for Health Promotion and Education, *Shaping the future of health promotion: priorities for action.* Health Promotion International, 2007. **23**(1): p. 98-102.

58. Leeuw, E.d., K.C. Tang, and R. Beaglehole, *Ottawa to Bangkok -- Health promotion's journey from principles to 'glocal' implementation.* Health Promotion International, 2007. **21**(1): p. 1-4.

59. Skinner, S., *Building community strengths: a resource book on capacity building.* 1997, London: Community Development Foundation Publications.

60. Smith, B.J., *WHO Health Promotion Glossary: New terms.* Health Promotion International, 2006. **21**(4): p. 340-345.

61. Rohrbach, L.A., et al., *Diffusion of school-based substance abuse prevention programs. .* American Behavioral Scientist, 1996. **39**(7): p. 919-934.

62. Kelder, S.H., et al., *Long-term implementation of CATCH physical education.* Health Education and Behaviour, 2003. **30**(4): p. 463-75.

63. Osganian, S.K., G.S. Parcel, and E.J. Stone, *Institutionalization of a school health promotion program: Background and rationale of the CATCH-ON study.* Health Education and Behaviour, 2003. **30**(4): p. 410-417.

64. Ackerman, L., *Development, transition or transformation: the question of change in organisations*, in *Organisation Development Classics*, D. an Eynde, J. Hoy, and D. Van Eynde, Editors. 1997, Jossey Bass: San Francisco

65. Hamalainen, R., *Designing and evaluating collaboration in a virtual game environment for vocational learning.* Computers and Education, 2008. **50**(1): p. 98-109.

66. Squire, K., *Cultural framing of computer/games.* Game Studies, 2001.

67. Glazier, R., *How to design educational games*. 1973, Cambridge, MA: ABT Associations.

68. Rasmusen, E., *Games and Information: an introduction to game theory*. 2001, Malden, BA: Blackwell.

69. Alessi, S.M. and S.R. Trollip, *Computer-based instruction: methods and development*. 1991, Englewood Cliffs, NJ: Prentice Hall.

70. Charlton, J.P. and I.D.W. Danforth, *Distinguishing addiction and high engagement in the context of online game playing.* Computers in Human Behaviour, 2007. **23**: p. 1531-1548.

71. Choi, D. and J. Kim, *Why people continue to play online games: in search of critical design factors to increase customer loyalty to online contents.* CyberPsychology and Behaviour, 2004. **7**: p. 11-24.

72. Paraskeva, F., S. Mysirlaki, and A. Papagianni, *Multi-player online games as educational tools: facing new challenges in learning.* Computers and Education, 2010. **54**: p. 498-505.

73. Mayer, R.E., *A taxonomy for computer-based assessment of problem-solving.* Computer in Human Behaviour 2002. **18**(6): p. 623-632.

74. Baltra, A., *Language learning through cmputer adventure games.* Simulation and Gaming, 1990. **21**: p. 445-452.

75. Kafai, Y., *Minds in play: computer game design as a context for children's learning*. 1997, Hillsdale, NJ: Lawernce Erlbaum Associates.

76. Mishna, F., et al., *Interventions to prevent and reduce cyber abuse of youth: A systematic review.* Research in Social Work Practice, 2011. **(in press)**.

77. Mishna, F., et al., *Interventions for Children, Youth, and Parents to Prevent and Reduce Cyber Abuse*. 2009, Campbell Systematic Reviews.

78. Davidson, J., Martellozzo, E., & Lorenz, M., *Evaluation of CEOP ThinkUKnow Internet safety programme and exploration of young people's Internet safety knowledge*. 2009, Kingston University: London. p. 1-57.

79. Kruger, R., A., and M.A. Casey, *Focus Groups: A practical guide for applied research, 3rd ed*. 2000: Thousand Oaks, CA: Sage Publications.

80. Bostan, B. and S. Ogut. *Game challenges and difficulty levels: Lessons learned From RPGs*. in *In International Simulation and Gaming Association Conference*. 2009.

81. Dooley, J.J., T. Shaw, and D. Cross, *Student actions and mental health after cyber-bullying.* European Journal of Developmental Psychology, (in press).

82. Crick, N.R. and K.A. Dodge, *A review and reformulation of social information processing mechanisms in children's social adjustment.* Psychological Bulletin, 1994. **115**(1): p. 74-101.

83. Crick, N.R. and K.A. Dodge, *Social information-processing mechanisms in reactive and proactive aggression.* Child Development, 1996. **67**(3): p. 993-1002.

84. Orobio de Castro, B., et al., *Hostile attribution of intent and aggressive behavior: a meta-analysis.* Child Development, 2002. **73**(3): p. 916-934.

85. Mayeux, L. and A.H.N. Cillessen, *Development of social problem solving in early childhood: Stability, change, and associations with social competence.* The Journal of Genetic Psychology, 2003. **164**(2): p. 153-173.

86. Takahashi, F., S. Koseki, and H. Shimada, *Developmental trends in children's aggression and social problem-solving.* Journal of Applied Developmental Psychology, 2009. **30**(3): p. 265-272.

87. Livesly, W.J. and D.B. Bromley, *Person perception in childhood and adolescence*. 1973, London: Wiley.

88. Yeates, K.O. and R.L. Selman, *Social competence in the schools: Toward the integrative developmental model for intervention.* Developmental Review, 1989. **9**: p. 64-100.

89. Gutnick, A.L., et al., *Always connected: The new digital media habits of young children*. 2010: New York: The Joan Ganz Cooney Center at Sesame Workshop.

90. Kang, C. *Underage and on Facebook*. 2011 [cited 2011 27 June]; Available from: http://www.washingtonpost.com/blogs/post-tech/post/underage-and-on-facebook/2011/06/12/AGHKHySH_blog.html.

91. Dooley, J.J., et al., *Aggression after traumatic brain injury: A theoretical approach.* Brain Injury, 2008. **22**(11): p. 836-846.

92. Cross, D., et al., *Australian Covert Bullying Prevalence Study (ACBPS)*. 2009, Child Health Promotion Research Centre, Edith Cowan University, Perth.

93. Dooley, J., et al., *Cyber-victimisation: The association between help-seeking behaviours and self-reported emotional symptoms in Australia and Austria.* Australian Journal of Guidance & Counselling, 2010. **20**(2): p. 194–209.

94. Dooley, J.J., et al., *Brain Quest: A novel approach to the measurement of social information processing.* Journal of Youth and Adolescence, under review.

95. Australian Communications and Media Authority, *Click and connect: Young Australians' use of online social media; 02: Quantitative research report.* 2009.