E-safety: the experience in English educational establishments

An audit of e-safety practices: 2005

Charlotte Barrow

Department of Education and Social Science

University of Central Lancashire

01772 893113

cljbarrow@uclan.ac.uk

Dr Gary Heywood-Everett

Department of Education and Social Science

University of Central Lancashire

01772 893109

Gheywood-everett@uclan.ac.uk

Acknowledgements

Contents

Tables

Charts

Executive Summary

This report presents the findings of research examining e-safety – the risks associated with the use of new technologies - in English schools and colleges in 2005. It is based on a survey of 444 schools, in-depth interviews with 61 teachers, a survey of 25 English Local Education Authorities (LEAs) and five Regional Broadband Consortia (RBCs). It examines:

- the technical safety measures being used in schools and colleges to reduce the risks to children
- policies and procedures that are currently in place to manage e-safety in educational environments
- programmes of e-safety education aimed at pupils, parents and teachers
- how schools and colleges access and use the support that is available to them
- models of good practice that reduce risk and could be shared with others.

It provides professionals concerned with e-safety in educational settings with an accurate and up-to-date review of the challenges posed by new technologies. Then, based on the strategies in evidence, it considers how these challenges may be addressed. This first section outlines some of the key findings of the research, offering recommendations for future policy and practice.

1. Having a designated Internet Safety Co-ordinator in place *and* having an Acceptable Use Policy (AUP) better equips teachers to deal with breaches of e-safety.

Some educational establishments are better equipped to deal with e-safety than others. Where there is an Acceptable Use Policy (AUP) *and* an Internet Safety Co-ordinator is in place, teachers report that they are better able to deal with breaches of e-safety. Half of all educational establishments surveyed did not have a designated Internet or E-safety Safety Co-ordinator (see Section 3.1) and many had not reviewed their AUPs recently. Risks to children may be reduced if educational establishments can address the growth in the use of new technologies and

any attendant risks within their AUP, and, where a designated individual can take responsibility for keeping others up to date.

2. Some educational establishments are not being provided with up-to-date support and advice about e-safety by their Local Education Authority (LEA).

Not all educational establishments' Acceptable Use Policies cover issues regarding emerging technologies, or technologies that are not permitted to be used in educational environments, despite evidence of widespread recreational use by pupils. The research suggests a key role for LEAs in this regard. Teachers report that they, and their pupils, need more advice about certain issues: up-to-date support and advice concerning the viewing of unsuitable online material (sites with pornographic, violent, racist or terrorist content); and bullying via chat rooms, email or websites (see Section 5.1.5). The current advice provided to educational establishments by LEAs does not necessarily reflect this need.

3. Some educational establishments are not being provided with up-to-date support and advice about e-safety by the British Educational Communications and Technologies Agency (Becta).

Teachers in Primary schools are less likely to use the support and advice offered by Becta than teachers in Secondary schools (see Section 3.1). All educational establishments are more likely to seek support and advice from their LEA than from Becta. Teachers' awareness of Becta and the support and advice it can provide may be limited and the Agency needs to address its lack of visibility in English educational establishments.

4. Breaches of e-safety are most likely to occur among the older pupils in both Primary and Secondary schools. The most common breach is the viewing of unsuitable online material. However, the research found that where pupils were taught about e-safety, all breaches of e-safety were reduced.

Overall, breaches of e-safety occur most commonly in Year 6 of Primary school and in Years 10 and 11 of Secondary school (see Section 5.1). The patterns of breaches of e-safety suggest that pupils are more vulnerable in specific school years. Some risks associated with e-safety are age and gender specific, for example, risks such as contact with inappropriate persons (often termed 'grooming') are rare, but most often affects girls in Year Nine, whereas plagiarism peaks in Years Six, Ten and Eleven – as pupils prepare for crucial tests or examinations and is more common among boys. Therefore, the risks children face and the support educational establishments require to deal with them may be predicted to some degree.

5. Breaches of e-safety are more likely to occur in educational establishments where pupils are allowed to bring their own personal equipment on to the premises (such as laptops, portable storage devices, etc.). In some cases, such as incidents of bullying via mobile phone, breaches are not only more likely to occur, but also occur with greater frequency when mobile phones are allowed on the premises.

The research suggests the need to consider what equipment is allowed on to educational premises and how this may increase the risk of breaches to e-safety. The risks could be reduced by a more careful consideration of what equipment is allowed and the contexts in which it can be used. Educational establishments may be inadvertently increasing their exposure to breaches of e-safety and be compounding the risks pupils face as a result of the lack of clarity around personal equipment use. This then raises tensions around the positive educational capabilities of new technologies and any potential negative impacts.

6. Teachers ability to deal with breaches of e-safety varies according to the training and support they receive, the policies and procedures in place in schools and the effectiveness of technical systems.

The extent to which teachers are equipped to deal with breaches of e-safety and the risks these pose to pupils varied across educational establishments. Although some had clear policies and procedures in place

to manage e-safety, coupled with training, support and technical systems that teachers' perceived to be effective, many did not. The research points to clear gaps in the strategic management of e-safety in English educational establishments and suggests that the risks associated with breaches of e-safety can be directly reduced by adopting coherent strategies.

Recommendations

1. A strategic and integrated approach towards e-safety is required in educational establishments.

E-safety needs to become integrated into educational establishments through a range of measures to ensure that it is addressed in an holistic manner. This could be done in three key ways;

- E-safety should be referred to in behavioural, anti-bullying, and child protection policies, as well as being part of every home-school agreement, so that awareness is raised amongst all members of the school community.

- One member of staff should act as designated Internet or E-safety Co-ordinator. This person would have responsibility for maintaining and monitoring strategies and systems to ensure that e-safety remains a priority.

- E-safety needs to be integrated into the curriculum, with direction and materials provided for teachers across all key stages and sectors.

2. A publicity campaign is needed to increase the visibility of Becta in English schools and colleges.

Teachers and other key staff in educational establishments need to be made aware of the support, advice and resources available to them. The research shows that teachers are most likely to utilise their LEA in relation to e-safety issues.

Becta need to consider whether they want educational establishments to access them directly, in which case they need to implement a high profile awareness campaign and ensure that they are able to cater for any subsequent increase in demand for their services. Alternatively, Becta could choose to channel resources through LEAs so that teachers benefit from Becta's expertise at a local level.

3. Issues relating to mobile technologies and e-safety need to be addressed in teaching and learning.

The research has found that where pupils are taught about e-safety, breaches of e-safety are reduced. Thus, to avoid, or exclude, teaching about new mobile technologies is to deny both the inevitable evolution of technology and the proven recreational use of these technologies by young people. Teaching materials need to be regularly reviewed in the

light of emerging technologies in order to prevent pupils being placed at increased risk.

4. Monitoring e-safety in English educational establishments should be facilitated by LEAs

In order to gain a greater understanding of the challenges faced by teachers responsible for e-safety, more effective monitoring of the situation in educational establishments is required. LEAs may be best placed to carry out this task, particularly paying regard to any relationship between the efficacy of e-safety strategies and the prevalence of e-safety breaches.

5. Targeted directives are required to counter breaches of e-safety amongst particular pupil groups.

The research shows that some pupils are more likely to be involved in breaches of e-safety than others. Pupils most commonly involved are those at the higher end of the school age range (i.e. Year 6 Primary and Years Ten and Eleven Secondary). Breaches are also influenced by gender, for example, girls are predominantly involved in incidents of bullying via mobile phones, whereas boys are more involved in incidents of plagiarism and the viewing of unsuitable online material. Therefore, strategies could be targeted specifically at groups of pupils based on known risks. Such an approach would protect pupils and reduce the problems associated with breaches of e-safety for staff.

6. Educational establishments need to consider alternative ways of managing the use of personal equipment brought onto their premises by pupils.

Although it is important not to overstate the tensions between the use of new technologies inside and outside school, the findings of this study show a clear association between the use of personal equipment on educational premises (e.g. laptops, mobile phones) and breaches of safety. That is, permitting the use of certain equipment or devices may increase risk. Therefore, educational establishments may need to develop new approaches to monitoring the appropriate use of such technologies on their premises.

7. Teachers require support that is tailored to their existing levels of expertise, but that takes account of the increased capabilities and uses of new technologies

The research found that the support provided to and used by teachers varied in terms of its quality and relevance to their needs. The provision of such support (for example, programmes of education) was variable and more likely to be implemented in Primary schools. The needs of teachers should act as the starting point for a comprehensive training programme in e-safety, made available contingent on teachers' needs as opposed to their designated roles and responsibilities.

1.0 Introduction

1.1 Aims of the study

This study was commissioned by Becta (the British Educational Communications Technology agency) in August 2005 to conduct an audit of the current level and range of activity within English state maintained educational establishments to ensure the safe and effective use of information and communication technologies (ICT).

In conjunction with Becta, the researchers drew up the following objectives for the study, which would;

1. Identify and ascertain the kinds of technological tools being utilised by educational establishments in order to minimise risks associated with the use of ICT

2. Critically analyse educational establishments' approaches to and provision of e-safety related programmes of education and other initiatives aimed at pupils

3. Examine educational establishments' policies and procedures in relation to e-safety

4. Critically analyse educational establishments' approaches to and provision of e-safety related programmes of education aimed at teachers and parents and other members of the school community

5. Evaluate the current levels of support and resources provided by a number of Local Education Authorities

6. Identify good practice and enable this to be shared with other educational establishments and relevant stakeholders

Those familiar with the broader agenda of work occurring in this area, will note that the terminology has evolved from 'internet' safety, to 'e' safety. This change in terminology reflects the fact that the risks associated with children and young people's uses of technology are not limited to their use of the Internet.

1.2 Background

The DfES (Department for Education and Skills), through Becta, have been recommending a range of strategies to educational establishments

to ensure the safety of their pupils (and other users) whilst using ICT since 1998[1]. Such recommendations need to be informed by a broad knowledge base, which can only be achieved through robust and contemporary research which monitors the climate in educational establishments as technologies evolve.

1.3 Previous research

In 2002, Becta commissioned an audit of internet safety practices in English schools, which is referred to where relevant in this work. This research was conducted by Wishart et al and has acted as a useful starting point in informing the design of this research study.

Key findings from Wishart et al's research included;

- 95 per cent of respondents had Internet filtering systems in place
- Only 20 per cent of teachers reported that they referred to the DfES's Superhighway safety resource
- The most frequent breaches of Internet safety involved pupils *accidentally* accessing inappropriate material online
- 89 per cent of teachers reported having an internet safety policy in place
- The issue concerning most schools was the accessing of inappropriate material
- 85 per cent of teachers reported that they taught pupils about internet safety
- Schools' most frequently cited future concern was regarding pupils' increased use of email

1.4 The approach taken in this research

The focus of the research here has shifted somewhat in order to keep abreast of changes in both the capabilities of technological devices, and the developing knowledge of professionals in this field about the negative ways in which technologies can be used as a vehicle for exploitation of children.

---

[1] http://safety.ngfl.gov.uk/schools/

1.5 This report

The findings presented in this report are organised according to three key themes which were identified in Becta's 2005 publication, *'E-safety: Developing whole school policies to support effective practice'*:

1. Schools' infrastructures in terms of policies and procedures

2. Technical measures schools may have in place

3. Pedagogical approaches aimed at implementing effective programmes of education.

It should be borne in mind that whilst findings from FE providers, Pupil Referral Units and Special schools are presented in this report, these are intended to provide a snapshot of the practices employed in these educational establishments, and are not presented here as an unequivocal representation of the policies and practice in these schools due to the small sample size of these establishments. In general, unless specified otherwise, the term 'educational establishments' in this report encompasses Primary schools, Secondary schools and those mentioned above.

Another key point that readers should take into account is the fact that the findings presented here reflect the experiences and strategies of those teachers who had an interest in the issue of e-safety, and were *able* to answer the questions posed to them. The low return rate of questionnaires (a total of 444 questionnaires were returned from 2812 sent out) suggests that some teachers simply may not be in a position to provide information about their e-safety policies and practices, for whatever reasons that may be.

2.0 Methodology

The research took place between September and December 2005 and had three main strands:

- a quantitative postal survey of schools and colleges of Further Education (n=444)
- a quantitative postal survey of Local Education Authorities and Regional Broadband Consortia (n=30)
- in-depth telephone interviews with teachers in 61 schools and colleges (n=61).

For ease of analysis the strands were divided into two Phases; Phase One being solely survey based; and Phase Two the detailed and more qualitative investigation. The principle was to explore the main aims of the research (set out above) with a representative sample of each type of establishment, selected at random from a national dataset. The achieved sample (set out in Table 2.1 below) is thus weighted towards Primary schools to reflect the greater proportion of Primary to Secondary, with other educational establishments included so as not to exclude settings where specific challenges around securing e-safety (such as fiscal resources or size or roll) may be present.

Table 2.1 Achieved sample

PHASE ONE	Number	Per cent
Primary schools	303	68
Secondary schools	123	28
Pupil referral units	8	2
Special schools	6	1
Colleges of Further Education	4	1
Total	**444**	**100**
PHASE TWO	Number	Per cent
Primary schools	42	69
Secondary schools	13	22
Pupil referral units	2	3
Special schools	2	3
Colleges of Further Education	2	3
Total	**61**	**100**

The basic aim of the sampling strategy was to gain returns from three Primary schools and one Secondary school in each of 135 English LEAs, these being selected at random from all LEAs. The achieved sample was

below that desired by 24 per cent at Phase One, but equalled that desired at Phase Two. The total number of schools and other providers contacted exceeded the achieved sample by a factor of four at Phase One and by 15 per cent at Phase Two. At each stage of the process random sampling procedures were used to identify replacement educational establishments. The procedures through which the sample was achieved are set out in detail in Appendix One of this report.

Incentives were used to secure participation in the research. At Phase One all of the returned surveys were entered into a prize draw and seven educational establishments were drawn at random and won ICT equipment for their school. At Phase Two all participating teachers were given a gift voucher for taking part in a telephone interview.

The data collected was in two main forms and this influenced its analysis. The quantitative data (elicited by the surveys) was coded and analysed using SPSS, a statistical analysis package. In addition to the quantitative data, teachers also provided some qualitative data in the form of their open responses to survey items. This data was coded and analysed manually, primarily to develop themes to add context to, and increase the understanding of, the quantitative data. The telephone interviews were recorded and transcribed. These elicited both quantitative and qualitative data and the same analytical procedures were used, with more weight to open coding responses and examining key themes in e-safety.

For a full outline of the procedures followed in relation to the sample, see Appendix One.

3.0 E-safety policies and procedures

This section focuses upon the range of policies and procedures that exist in schools and colleges in order to reduce the level of risk that pupils are exposed to through their use of ICT. It examines any training teachers have received in relation to e-safety, the sources of information and advice they use (and its perceived efficacy), the capacity of organisations to deal with breaches of e-safety, the development and role of Acceptable Use Policies (AUPs) and the role of the e-safety Co-ordinator. The section concludes by setting out the main findings of the research in relation to e-safety policies and procedures and how they may reduce risk.

3.1 Internet safety / e-safety co-ordinators in schools

As new technologies have developed and have been used increasingly in teaching and learning contexts, the issue of e-safety has taken on greater significance in schools and colleges. In 2005, the British Educational Communications and Technology Agency (Becta) recommended that, in order to best cope with the challenges posed by new technologies, a person with responsibility for *internet* safety should be identified and that person (preferably a senior manager) should take the post of internet safety co-ordinator.

This research found that 47 per cent of teachers reported that their educational establishment had a designated Internet Safety Co-ordinator, and that figure was relatively constant across organisations. For example, half of Special schools, Pupil Referral Units and colleges of Further Education had an Internet or E-safety Co-ordinator, compared to 48 per cent of Secondary schools and 43 per cent of Primary schools. Half of the teachers reported that their educational establishment did not have an Internet or E-safety Co-ordinator, and three per cent were unsure.

The breakdown of educational establishments that had a designated Internet or E-safety Co-ordinator by school is set out in Table 3.1 below.

Table 3.1 Educational establishments with a Designated Internet or E-safety Co-ordinator

	Number	Per cent
Primary school	144	48
Secondary school	53	43
Special school	3	50
Pupil referral unit	4	50
Further education	2	50

Secondary schools are marginally more likely to have a designated Internet Safety Co-ordinator than Primary schools, but this difference is of little significance.

Where the Internet or E-safety Co-ordinator was also the individual completing the survey (in 68 per cent of all schools and colleges), additional data was collected. This shows that in almost half of all educational establishments the Internet or E-safety Co-ordinator was also head of ICT, in a quarter of cases she/he was a classroom teacher and in only 21 per cent of cases were they a senior manager (such as head, principal, deputy head, or member of the senior management team). Thus, responsibility for e-safety has been delegated to an individual in only half of all educational establishments and to a senior manager in only a quarter. Moreover, e-safety concerns (including, but extending beyond concerns with the use of the internet) were reported to this individual in 85 per cent of educational establishments. This suggests that e-safety remains an issue firmly located within ICT departments, is primarily the responsibility of those responsible for ICT and is possibly somewhat 'detached' from senior managers.

3.2 The development and role of Acceptable Use Policies (AUP's) in educational establishments

Acceptable Use Policies are documents (often agreements or codes of conduct) which outline the ways in which various technologies should, and

should not be used within a learning environment. The nature and scope of these can vary significantly between educational establishments and the role they play in promoting e-safety remains somewhat unclear.

3.2.1 Educational establishments with an AUP in place

The research found that the majority of educational establishments (85 per cent) currently have an AUP in place (a similar figure, 89 per cent, was reported by Wishart et al in 2002). However, the presence of a designated Internet Safety Co-ordinator may affect the development of an AUP; 92 per cent of educational establishments with an Internet or E-safety Co-ordinator have an AUP, compared to 78 per cent of those without such an individual.

3.2.2 Development of the AUP

In the majority of cases (73 per cent) the Head or Principal was involved in drawing up the AUP and in over half of all cases the Senior Management Team played a part. However, in only 16 per cent of cases was the Child Protection Liaison Officer included and in 15 per cent the Special Educational Needs Co-ordinators (SENCO). This suggests a high degree of strategic commitment to the AUP, but points to some weakness around the lack of involvement of professionals with a key role around the protection of particularly vulnerable children.

However, examples of good practice which included staff in the development of AUPs were identified amongst some educational establishments that participated in Phase Two of the research, as shown by this excerpt from a teacher below:

"The guidelines that the staff adhere to were set up in consultation with the school staff, including NTA's. All staff are aware of the guidelines when they're updating. This is also in consultation with the Governors."

Urban Primary school

With regards to the sources used by educational establishments in developing AUPs, the research also found that colleges of Further Education and Pupil Referral Units were more likely to seek guidance around the content of the AUP than Primary, Secondary and Special schools. Moreover, *all* colleges sampled had sought guidance on content

from the Joint Information Systems Committee (JISC), suggesting an effective single source. However, the primary source of guidance (including that for content), for schools was their Local Education Authority (LEA), as opposed to specialist bodies such as Becta, their Regional Broadband Consortia (RBCs), children's charities or the Department for Education and Skills (DfES). When Becta guidance was sought, it was most commonly used to locate a sample AUP (reported by 33 per cent of schools).

3.2.3 Issues covered by AUPs

Teachers were asked what issues or areas their educational establishments' AUP covered. These are shown in the table below (see Table 3.2).

Table 3.2   AUP coverage

Issue covered	Per cent
Use of World Wide Web	98.5
Use of email	95
Downloading files or images	74
Use of CDs/disks in school	65
Use of chat rooms	64
Use of message boards/web logs	42
Use of personal devices in school	35
Bullying via ICT	32
Use of web cams/video conferencing	22
Use of mobile phones (text messages and calls)	10
Use of mobile phones (camera and video)	8
Other (.g. copyright issues, fax use, memory sticks, etc.)	2.4

It is clear that in most educational establishments, the AUP focuses on World Wide Web and email, with some evidence that emerging technologies are being addressed. Only a minority of AUPs include the use of message boards or web logs and an even smaller minority cover the use of personal devices, bullying via ICT and the use of mobile phones. This could suggest that AUPs are not keeping up with new technologies and could be overtaken by new developments. However, there may be a limited ability of educational establishments to accommodate change. Comparing the findings with Wishart et al's research (2002), shows that coverage of the World Wide Web, email and chat rooms in AUPs has

increased, possibly as a result of greater awareness of children and young peoples' use of these technologies.

3.2.4 Committing to the AUP

The main signatories to the AUP (those who are required to sign it, or confirm that they will adhere to its principles) are parents and pupils. Almost 80 per cent of teachers reported that parents and pupils are required to sign the AUP.

Wishart et al's 2002 study found that 51 per cent of parents and 49 per cent of pupils were asked to sign an AUP, so the increased figures found by this research may suggest that more educational establishments are recognising the need to make pupils and parents aware of the significance of a safety policy, as demonstrated by this excerpt from a teacher participating in Phase Two of the research;

"as every child enters the school they take home internet permission slips which have our rules for safe use of the internet which they and their parents sign. That comes back to the school, so we keep a copy of that for every child. If it's not signed by the parents we don't let them use the internet"

Urban Primary school

In under half of educational establishments, all of the staff (including support staff) are required to sign the AUP and only 11 per cent of teachers reported that adults using facilities out-of-hours have to sign the AUP, indicating some potential gaps in its use as a measure to promote and secure e-safety in environments which aim to increase access to ICT in communities.

3.2.5 Association of AUP with other school policies

Teachers were asked if their AUPs had links to other policies and the majority (53 per cent) reported that it did not, that it is a discrete policy document. This suggests that e-safety may be a high priority, but could lack coherence across educational establishments, again being located within a specific area of teaching and learning.

In summary, the main issues around the development of AUPs are:

- There is a greater likelihood that an AUP will be in place in educational establishments with a designated Internet or E-safety Co-ordinator
- An AUP may not keep up with the development of new technologies (such as web logs and mobile phones)
- Some teachers lack awareness of the guidance that is available to assist them in the development of such policies
- There is high strategic commitment to AUPs, but potential gaps regarding the inclusion of others with responsibilities for, or an interest in children at risk
- Some AUPs do not cover the use of new technologies on educational premises.

In most educational establishments the challenge may be to support teachers in developing AUPs that address these issues, drawing on the guidance offered and available from a range of sources. The experience of those teaching within colleges of Further Education and the role of JISC may be useful to examine in some respects.

3.3 The revision of AUPs

In its guidance Becta (2005) recommends that e-safety policies "should be embedded within a cycle of establishment, maintenance, ongoing review, modification, reporting and annual review" (2005: 9-10). With this in mind, the research examined the extent to which AUPs had been modified (or even abandoned entirely), to gauge how frequently such reviews take place, or if they take place at all.

Although only 31 per cent of teachers reported that they revised their policy annually, a higher proportion (78 per cent) reported that they had revised their AUP within the last year. The survey found that just over half (52 per cent) of all educational establishments had revised their AUP since its initial development. Of these, almost 70 per cent reported that their AUP had been developed prior to 2002, suggesting that guidance (above) was being followed by some educational establishments, but not others. To examine whether there was any statistical substance to the findings, a research hypothesis related to the modification of AUPs was designed and tested:

Testing research Hypothesis 3.1: Examining the utility of AUPs over time
In order to examine the development of AUPs, when the AUP was implemented and when it was revised, a research hypothesis was designed and tested.

Hypothesis 3.1:	Educational establishments that implemented an AUP prior to 2002 are more likely to have revised it by 2005 than educational establishments that developed their AUP in 2002 or later.
Test:	Mann Whitney test
Result:	z=-4.588; p=0.000 (p<0.01)
Summary:	As educational establishments with an AUP implemented prior to 2002 are statistically more likely to have revised it than educational establishments that have an AUP which was implemented in 2002 or later, the above hypothesis was accepted.
Comment:	Accepting hypothesis 3.1 suggests that the utility of an AUP is limited over time, and they may require revision.

Thus, the research suggests that, regardless of whether Becta advice is followed or not, AUPs may have a maximum useful lifespan of two to three years. Consequently, some educational establishments are currently using an AUP that is out of date.

In summary, the main issues around the revision of AUPs are:

- AUPs are being revised (as recommended by Becta), but not as frequently as recommended or with equal frequency across all educational settings
- AUPs may have a useful lifespan of two to three years
- Some educational establishments have AUPs that are out of date.

In educational establishments the challenge may be to raise teachers' awareness of the need to revisit and possibly revise their AUP on a regular basis.

3.4 Perception of the AUP as an e-safety measure

The survey examined teachers' perception of the AUP as an effective e-safety measure, in terms of it being a measure that reduced risks to children in teaching and learning contexts. It found that very few teachers (11 per cent) feel that AUPs do *not* reduce risks and the majority (78 per cent) feel that they do. However, of this figure, only 13 per cent reported that they reduce risk significantly, suggesting that AUPs may be perceived as an important part of a *wider* strategy of risk reduction, i.e. they may not be a sufficient strategy if used only on a standalone basis.

The research identified a degree of variance between the views of teachers in Primary and Secondary schools and this was examined further to determine if any difference was statistically significant.

Testing research Hypothesis 3.2: Examining teachers' perceptions of AUPs in Primary and Secondary schools

In order to examine teachers' perceptions of their AUP as an e-safety measure, a research hypothesis was designed and tested statistically.

Hypothesis 3.2: Teachers in Primary schools are more likely than teachers in Secondary schools to regard their AUP as an e-safety measure which reduces risks to children.

Test: Mann Whitney test

Result: $z=-3.721$; $p=0.000$ ($p<0.01$)

Summary: As teachers in Primary schools are statistically more likely than teachers in Secondary schools to regard their AUP as an e-safety measure which reduces risks to children, the above hypothesis was accepted.

Comment: Accepting hypothesis 3.2 suggests that Primary school teachers are more likely to perceive AUPs as an effective e-safety measure than Secondary school teachers.

Thus, the research suggests that teachers' perceptions of AUPs may be framed by context, with those teachers in Primary schools more confident in the contribution of the AUP to risk reduction than teachers in other settings. In most settings (72 per cent), teachers reported that their AUP *has* lead to the more appropriate use of ICT, and a similar figure reported that they increase pupils' understanding of the safe use of ICT in educational establishments. However, when teachers were asked how

essential they felt the AUP was to the broader strategy of securing e-safety in schools and colleges, there were found to be differences linked to their role. For example, heads of departments and Deputy Heads are more likely to see AUPs as essential, whereas Network Managers, e-safety or ICT Co-ordinators are less likely to do so, possibly linked to their increased awareness of any limitations.

In summary, the main issues around teachers' perceptions of AUPs are:

- AUPs are less likely to be regarded as an e-safety measure that reduces risks to children in Secondary schools than in Primary schools
- AUPs have benefits beyond risk reduction, such as increasing pupils' appropriate use of ICT and raising their awareness of e-safety
- teachers with specialist ICT knowledge are less convinced that AUPs are an essential part of a broader e-safety strategy for educational establishments.

In most educational establishments the challenge may be to harness specialist knowledge to identify any weaknesses in AUPs and address the different perceptions of teachers across schools.

3.5 AUPs and dealing with e-safety in the educational environment

The research examined the extent to which AUPs play a significant role in terms of equipping teachers with effective strategies to deal with any breaches in e-safety. The majority of teachers (75 per cent), irrespective of whether or not there was an AUP in place, reported that they had effective strategies in place. However, comparison between settings where there was or was not an AUP showed some variation (see Chart 3.1 below).

Chart 3.1   **Effective strategies to deal with breaches of e-safety and presence of an AUP**
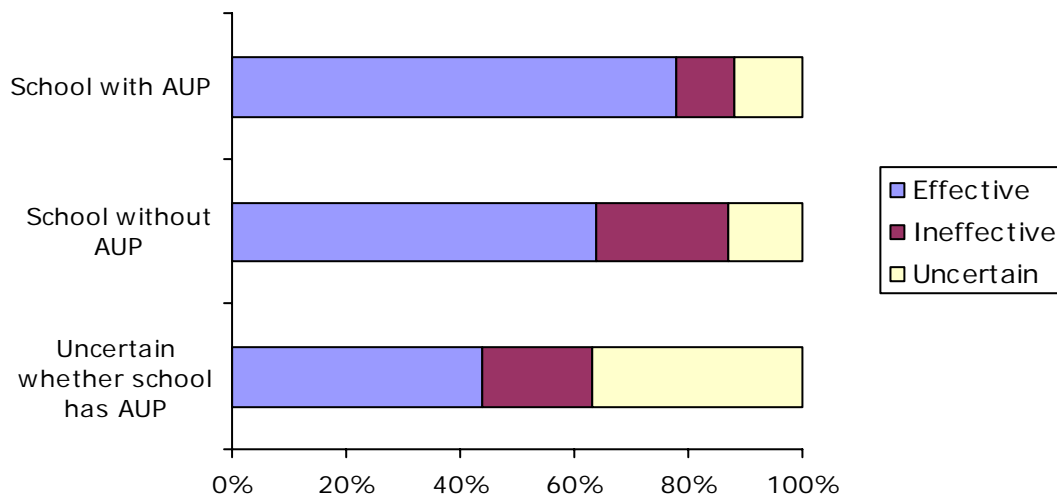
Teachers in educational establishments *without* an AUP are *less* likely to feel they have effective strategies in place and *more* likely to report that their strategies are ineffective. That is, an AUP appears to have a dual effect of equipping teachers with effective strategies around e-safety breaches and eliminating (or reducing the use of) ineffective strategies. Although the variance in both areas was below 13 per cent, this suggests that where an AUP is in place, strategies are more effective.

In order to further examine any relationships between AUPs and effective strategies to deal with breaches to e-safety, further analysis of the data was undertaken, specifically to examine the presence (and any influence of) an E-safety Co-ordinator. The presence of an Internet or E-safety Co-ordinator has a positive impact in terms of equipping teachers with effective strategies to deal with any breaches in e-safety, only slightly less so than the presence of an AUP. The extent to which e-safety Co-ordinators lead to the possible elimination or reduced use of ineffective strategies is marginal, compared to the presence of an AUP (see Chart 3.2 below).

Chart 3.2 **Effective strategies to deal with breaches of e-safety and educational establishments with a designated Internet Safety Co-ordinator**
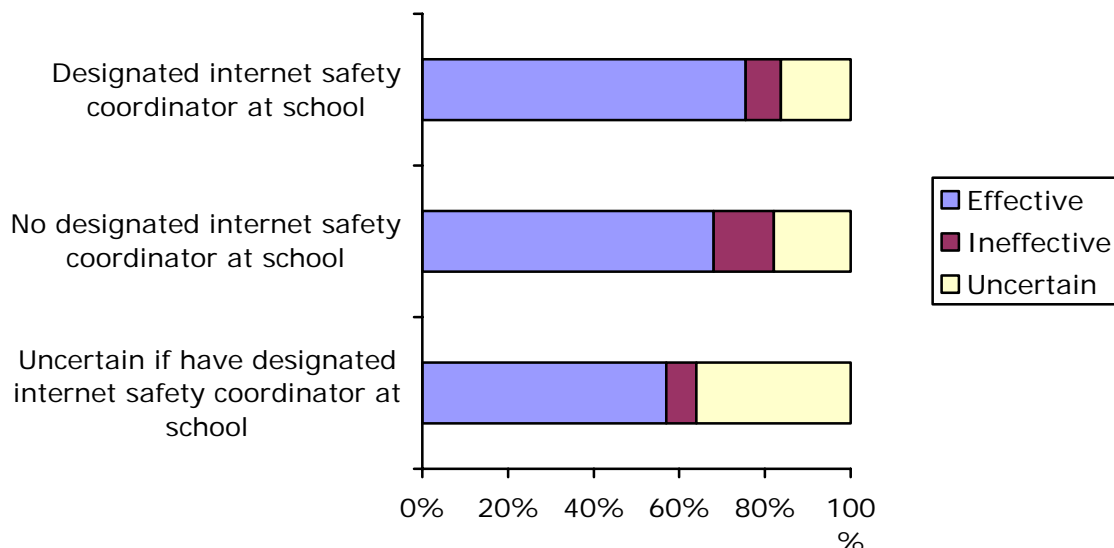
The majority of teachers involved in the research (85 per cent) felt able to deal with e-safety issues, although heads of departments and Deputy Heads report that they are better equipped than classroom and head teachers. The research identified variance in the extent to which teachers felt equipped to deal with issues related to e-safety between those who feel supported by their LEA and those who do not. To determine if any difference was statistically significant a hypothesis was designed and tested:

Testing research Hypothesis 3.3: Examining the support provided by LEAs in relation teachers' ability to manage e-safety

In order to examine teachers' ability to manage issues of e-safety in relation to whether or not they feel appropriately supported by their LEA, a research hypothesis was designed and tested statistically.

Hypothesis 3.3: Teachers who report being able to manage issues related to e-safety at their school are more likely to feel appropriately supported by their LEA than those who do not feel able to do so.

Test: Mann Whitney test

Result: z=7.531; p=0.000 (p<0.01)

Summary:	As teachers who reported being able to manage issues related to e-safety are statistically more likely to feel appropriately supported by their LEA than those who do not feel able to do so, the above hypothesis was accepted.
Comment:	Accepting hypothesis 3.3 suggests that receiving appropriate advice and support from LEAs is key to raising teachers' ability to manage e-safety.

Thus, teachers feel better equipped to deal with issues of e-safety when they are appropriately supported by their LEA. Irrespective of the presence of an Internet or E-safety Co-ordinator, or an AUP, the research suggests that *support* may equip teachers to better deal with e-safety.

In summary, the main issues around AUPs and e-safety in the learning environment are:

- AUPs may equip teachers with more effective strategies to deal with breaches in e-safety and reduce the use of ineffective strategies
- The presence of an Internet or E-safety Co-ordinator may also equip teachers with more effective strategies to deal with breaches in e-safety – and this could be investigated further
- The support of LEAs may be a central factor in increasing teachers' ability to manage e-safety.

In educational establishments it would be useful to identify the support that is currently equipping some teachers with greater ability to manage e-safety, in order to extend this to colleagues.

3.6 Dealing with disclosures

When an e-safety incident occurs, regardless of where it takes place, a child may disclose details of the incident at school. The research sought to assess the impact of school policies and procedures on dealing with disclosures; i.e., whether teachers are equipped to deal with such incidents in an effective and appropriate manner.

The research found that over half of teachers (59 per cent) feel that their school *has* appropriate measures in place to deal with disclosures around e-safety issues, but a significant minority (25 per cent) were unsure. Where an educational establishment had an AUP, more teachers report that appropriate measures are in place and fewer are unsure. In settings

where an E-safety Co-ordinator is in place teachers are also more likely to report that they have appropriate measures in place.

Only half of the teachers participating in the research feel that their LEA offers appropriate advice and support and advice to deal with such breaches – a clear gap in support. However, further interrogation of the data shows that this may be linked to awareness and use of such advice and support. For example, those teachers who had used such support were twice as likely to report that it was appropriate. The majority of those who had not did not report that it was inappropriate, but that they were unsure. These findings concerning the issue of disclosure add further weight to the emerging theme from this research, that teachers in educational establishments with a number of strategies in place, supported externally, may be better equipped to deal with breaches of e-safety. AUPs are therefore an important, but not free-standing element of any effective strategy to promote e-safety.

In summary, with regard to the issue of AUPs and other such policies in educational establishments, the research points to the need to view these policies in a wider context of strategies and support available to teachers. The research identifies clear (and in some cases statistically significant) links between teachers' ability to manage e-safety and the appropriateness of the support they receive. It shows that AUPs are context specific, with different value assigned to them and their potential limitations more and less understood by teachers. It suggests that AUPs cannot cope with new technological developments without review and revisions and that their contribution to e-safety, alongside other strategies, such as the identification of an e-safety Co-ordinator, is largely positive.

3.7 Sources of advice used by teachers

One of the aims of the research was to examine whether those tasked with providing support and advice to teachers on e-safety matters were doing so effectively, and what needs still exist. Teachers were asked to identify (and rate) the sources of advice or information they had used in relation to a number of areas, including the development of their AUPs and the information they provided to staff.

3.7.1 Current sources of support and advice

The research found that teachers' primary and current source of support and advice (where they go to first and where they go to now) concerning

e-safety is their LEA, reported by 61 per cent of teachers. A quarter of the sample reported that Becta is their current source, with 12 per cent going to their own Head and 13 per cent using the DfES. Very few teachers reported that they currently use their Internet Service Provider (ISP), an internet safety organisation or children's charity (three per cent or less in each case). Teachers in Secondary schools are much more likely to use Becta and the DfES and those in Primary schools are more likely to use their LEA. Teachers in Pupil Referral Units use their ISP more than any other teachers, possibly indicating a lack of other support or awareness of it. The main source of additional support and advice is 'in-house', from the ICT department or the E-safety Co-ordinator, reported by 58 per cent of teachers.

Disregarding where teachers' primary and current source of advice and support lies, the research found that in the past, the most frequent source used by teachers was once again their LEA (used by 74 per cent of teachers), followed by Becta (49 per cent of teachers) and the DfES (40 per cent of teachers). Under a third of the sample reported that they had used in-house support and almost 20 per cent their ISP, or an internet safety organisation. At some time, ten per cent of the teachers had used a children's charity, suggesting that they may play a specialist, but important role.

3.7.2 Support and advice provided by Becta

The research found that the support and advice teachers' sought from Becta was linked to where they work. For example, teachers in Secondary schools are more likely to go to Becta than Primary schools (31 per cent Secondary schools, 11 per cent primary schools). Primary schools are particularly less likely to go to Becta to obtain resources in teaching pupils about e-safety, which is particularly surprising as Becta have had an Internet Proficiency Scheme for Key Stage 2 pupils available since 2003.

To see if this difference was statistically significant, a research hypothesis was designed and tested:

Testing research Hypothesis 3.4: Examining the use of Becta's e-safety advice in Primary and Secondary schools

---

In order to examine the use of Becta's e-safety advice in Primary schools compared to Secondary schools, a research hypothesis was designed and tested statistically.

Hypothesis 3.4:   Primary school teachers will be less likely to use Becta as a source of e-safety advice than Secondary school teachers.

Test: Mann Whitney test

Result: z=-4.058; p=0.000 (p<0.01)

Summary: As Primary schools teachers will be less likely to use Becta as a source of e-safety advice than Secondary schools, the above hypothesis was accepted.

Comment: Accepting Hypothesis 3.4 suggests that Primary school teachers may be statistically less likely to use resources provided by Becta as a source of e-safety advice.

This indicates a clear need to extend the take-up of the support and advice offered to teachers in Primary schools by Becta, possibly by raising teachers' awareness of it, or making it more amenable to them. Given that the survey was weighted towards Primary schools (to reflect the national distribution of schools), the difference and its statistical significance suggests that current support and advice may be skewed towards teachers in Secondary schools.

In order to see if the disproportionate use of Becta by Secondary school teachers was linked to other factors, such as their level of e-safety awareness, evidenced by the presence of an Internet or E-safety Co-ordinator, another hypothesis was designed and tested:

Testing research Hypothesis 3.5: Examining the use of Becta's advice in schools and the presence of a dedicated e-safety Co-ordinator

In order to examine the use of Becta's e-safety advice in educational establishments with or without a dedicated e-safety Co-ordinator, a research hypothesis was designed and tested statistically.

Hypothesis 3.5:   Educational establishments with a dedicated e-safety Co-ordinator will report greater use of the advice provided
by   Becta than educational establishments without a dedicated e-safety Co-ordinator.

Test: Mann Whitney test

Result:	z=-1.314; p=0.189 (p>0.05)
Summary:	As educational establishments with a dedicated e-safety Co-ordinator are not statistically more likely to report greater use of the advice provided by Becta than educational establishments without a dedicated e-safety Co-ordinator, the above hypothesis was rejected.
Comment:	Rejecting Hypothesis 3.5 suggests that the presence of a dedicated e-safety Co-ordinator may not statistically affect the use of Becta's advice in schools.

This suggests that Becta's advice is not necessarily skewed towards the 'e-safety aware', but is accessed by those with differing levels of awareness. The significance of this statistical difference is that it undermines the possibility that teachers' take-up of Becta support and advice may be skewed to Secondary schools *because* the teachers there are more conscious or aware of e-safety issues (albeit assessed by the proxy measure of the presence of an e-safety Co-ordinator). That is, *the presence of an E-safety Co-ordinator* (*if* this can be used to assess awareness of e-safety issues) *makes no statistical difference to the take-up of advice provided by Becta* – other factors may be implicated.

The perceived quality of the support offered by Becta was explored further in Phase Two of the research (61 in-depth interviews with teachers). These interviews found that overall, 47 per cent of teachers feel well supported by Becta and few (ten per cent) report poor or very poor support. Perhaps significantly, those most likely to access support (teachers in Secondary schools) report lower levels of satisfaction. The contradiction within these findings, point to some interesting possibilities. One of these is that Becta offers support and advice disproportionately to teachers and perception of quality may be linked to availability, that is, teachers in Primary schools may feel well supported in the context of lower levels of availability – but the research does not support this interpretation conclusively.

3.8 Support and advice provided by LEAs or RBCs

The support and advice offered to teachers by their LEA and RBC was examined in detail through the research. In particular, it assessed support offered to teachers in the development of their AUP, but also that provided with regard to breaches of e-safety. In addition, LEA officers

(n=25) and RBC officers (n=5) completed a survey around their role in relation to e-safety in English educational establishments. The research was thus able to develop a picture of support from both provider and user perspective, linking it to policy developments and risk reduction.

Officers in *all* of the LEAs sampled and in the majority of RBCs (80 per cent) reported that they currently provide support and advice for educational establishments' about e-safety policies and procedures.

3.8.1 Issues that LEAs and RBCs provide guidance and support about

All LEAs and RBCs reported that they provide sample AUPs and that these cover a range of issues (set out in Table 3.3 below).

Table 3.3   Issues covered in sample AUPs

Issue	LEAs (%)	RBCs (%)
Use of the www	96	50
Use of email	96	25
Use of chat rooms	80	50
Use of items brought into school	64	50
Use of Instant Messaging	60	50
Bullying via ICT	56	50
Use of portable equipment	56	0
Use of web cams	40	50
Use of video conferencing	36	50
Use of mobiles for pictures/ video	16	0
Use of mobiles for calling or texts	12	0
Other issues (e.g. legal issues)	4	25

It is clear that sample AUPs provided by LEAs and RBCs vary in terms of their coverage. Those provided by LEAs are generally more extensive (compared to RBCs), but there is great variance between LEAs. For example, where the majority of LEAs (80 per cent or more) provide sample AUPs that cover use of the world wide web, email and chat rooms, a minority (40 per cent or less) of LEAs provide samples that cover web cams, video conferencing and the use of mobile phones. A significant minority (44 per cent) do *not* cover bullying via ICT, or the general use of portable equipment, such as portable storage devices, games, CDROMS, etc.

The evidence of inconsistent and sometimes insufficient coverage of some e-safety issues in sample AUPs, specifically those linked to newer technologies and their use in educational establishments can be compared to teachers need for support and their reliance on LEAs in particular. For example, almost half of teachers seeking a sample AUP sought one from their LEA, but the issues covered in the sample vary by authority. Thus, the extent to which an AUP will cover any or all e-safety issues may be LEA contingent and some new technologies are not covered in up to 50 per cent of cases.

To examine the possible sources of variation in the issues covered in sample AUPs, participants were asked where the information contained within their sample AUPs was sourced. That is, where did they gain the information to pass on to others (i.e. teachers)?

The research found that the primary source of advice (see Table 3.4 below) for LEAs was Becta but for RBCs the primary source of advice was in-house expertise.

Table 3.4   Sources of advice used by LEAs and RBCs

Source of advice	LEAs (%)	RBCs (%)
Becta	80	25
In- house expertise	72	50
(other) LEAs or RBCs	68	25
DfES	56	25
Children's charities	44	25

Other common sources of advice used to inform sample AUPs are in-house expertise (in 72 per cent of LEAs) and advice provided by another LEA or RBC (68 per cent). This raises issues around the extent to which current LEA staff, or those in other LEAs may hold up-to-date knowledge (which they are circulating to others) about the risks posed to children by new technologies. The research could not ascertain whether it was a lack of awareness that led to omission of some key e-safety issues from sample AUPs or not. However, there was found to be no correspondence between those LEAs providing sample AUPs to schools that were partial in their coverage of e-safety issues and those LEA officers who reported seeking support from within their own LEA, or from other LEAs. This suggests that coverage may not be contingent on the source of advice, but may be linked to policy decisions taken within the LEA. For example, the research found that only 14 per cent of LEAs or RBCs provide information to

schools as a matter of course (to all educational establishments). Thus, the extent to which the provision of support and advice to teachers is given sufficient priority across English LEAs is not clear.

3.8.2 Support and guidance offered by LEAs and RBCs in relation to breaches of e-safety

The research also examined the support and advice offered by LEAs and RBCs around breaches of e-safety. Over half (53 per cent) of teachers reported that their LEA or RBC offers appropriate advice and support to deal with breaches of e-safety or risks that pupils may be exposed to through their use of ICT, a minority (eight per cent) felt they do not and the remainder are uncertain. Of those teachers who had actually used LEA support in relation to any breaches of e-safety, 62 per cent reported that it offered appropriate advice and support, suggesting that *using* the LEA increases satisfaction.

Because so many teachers involved in the research had used such advice and could make an assessment of its quality on the basis of using it, the following areas are where LEAs and RBC can be assessed as providing *good* support and advice to teachers:

- the intentional viewing of unsuitable online material (52 per cent)
- contact with potentially inappropriate persons – commonly termed grooming (34 per cent)
- attempts to breach the security system (26 per cent)
- bullying via websites, chat rooms or emails (21 per cent)
- bullying via mobile phones (16 per cent)
- inappropriate use of mobile phones (12 per cent)
- bullying via mobile phones (12 per cent)
- intentional plagiarism (nine per cent).

It is clear that the areas where LEAs and RBC provide teachers with the best support and advice (the most highly rated) are the same areas of expertise most commonly contained within sample AUPs. Fewer teachers reported that support was good regarding new technologies such as those associated with mobile phones. This could suggest that some LEAs lack the capacity to provide support and advice in some areas of e-safety and in cases where they do, its quality is not perceived to be high by its recipients. New technologies may be an area of e-safety where LEAs are both less *likely* to be able to offer support and where they are less *able* to offer good support.

3.8.3 Quality of the support and guidance provided by LEAs and RBCs

The research identified some apparent differences in teachers' perceptions of the appropriateness and quality of the support and advice provided by LEAs by sector, with teachers in Primary schools reporting greater levels of support than teachers in Secondary schools. To see if this difference was statistically significant, a research hypothesis was designed and tested:

Testing research Hypothesis 3.6: Teachers' perceptions of the advice and support their LEA provides to Primary and Secondary schools

In order to examine how teachers in Primary schools compared to teachers in Secondary schools feel about the e-safety advice and support they receive from their LEA, a research hypothesis was designed and tested statistically.

Hypothesis 3.6:	Teachers in Primary schools are more likely than teachers in Secondary schools to feel appropriately supported by their LEA's when dealing with e-safety.
Test:	Mann Whitney test
Result:	$z=-6.415$; $p=0.000$ ($p<0.01$)
Summary:	As teachers in Primary schools are statistically more likely than teachers in Secondary schools to feel appropriately supported by their LEA when dealing with e-safety, the above hypothesis was accepted.
Comment:	Accepting hypothesis 3.6 suggests that Secondary school teachers may need further support, or that the support that they currently receive is inappropriate to them.

This indicates a clear need to address the support and advice offered to teachers in Secondary schools by LEAs and RBCs, possibly by raising teachers' awareness of it, or making it more amenable to them. However, Primary school teachers may feel more adequately supported because of a reduced exposure to some breaches of e-safety (discussed further and in more detail in this report). That is, the difference could be because teachers in Secondary schools require *differentiated* support and advice and this is not, as evidenced above, being provided, or where it is, is not perceived to be wholly appropriate. The variance in teachers' perceptions may be linked to the extent to which some new technologies pose age-

specific risks. The absence of support around these may need to be addressed by LEAs.

3.9 Overall efficacy of LEA and RBC strategies to deal with e-safety

The LEA and RBC officers included in the research were asked to rate the effectiveness of their e-safety strategies. The majority (60 per cent) reported that they do have effective strategies to deal with breaches of e-safety, or, risks pupils may be exposed to through their use of ICT, 20 per cent reported that they do not and the remainder were uncertain. More specifically, regarding disclosures, less than a quarter of LEAs feel that they have appropriate measures in place to deal with these, compared to 60 per cent of RBCs. However overall, the majority of LEA and RBC officers felt that their organisation was well equipped to deal with issues related to e-safety, but were unsure as to how well equipped teachers in educational establishments were. Those within RBCs were slightly less confident of organisational ability, with 20 per cent reporting that their RBC was not well equipped. The majority of respondents within LEAs (76 per cent) reported that they had not received any training on e-safety issues.

3.10 Summary of the section

The research illustrates that a range of policies and procedures exist in educational establishments in order to reduce the level of risk that pupils are exposed to through their use of ICT. The sources of information and advice teachers use varies, as does its perceived efficacy and appropriateness. The capacity of organisations to deal with breaches of e-safety is contingent on both sector and location, with the development and role of Acceptable Use Policies (AUPs) showing wide variation in support and advice offered by LEAs and RBCs.

All of those involved in promoting or securing e-safety in educational establishments can find room for both optimism and concern in the

findings of this research. Addressing the following issues may secure greater e-safety:

- taking e-safety outside ICT and departmental locations and integrating a concern with it in the everyday practices and procedures in educational establishments
- appointing an E-safety Co-ordinator in educational establishments
- increasing the scope of AUPs and other e-safety policies to include the use of new technologies, building on the coherence achieved by bodies such as JISC
- addressing the geographical and sectoral variance in support offered to teachers and its perceived appropriateness
- increasing the take up of support and advice offered by Becta
- addressing the links between teachers' confidence to deal with e-safety issues and the support offered by LEAs
- providing training for LEA officers and increasing e-safety coordination between LEAs.

E-safety policies and procedures, as evidenced by this study of English educational establishments, are not coherent and in some cases may not address the risks posed to children by the increased use of new technologies in teaching and learning contexts.

4.0 Technical measures in place in schools

This section examines the technical measures and technical systems that schools have in place. It examines the use and adequacy of technical measures, disruptions caused by them and the technical support available to teachers. It also examines the technical equipment that pupils are allowed to bring in and use at school or college, examining any links between equipment use and disruption to teaching and learning. The research particularly explores technical filtering systems; Wishart et al (2002) found that the majority of schools had filtering of some sort in place, but this research examines in detail the impact of these systems upon teaching and learning, moving beyond the factual issue of whether technical measures existed or not, to explore the implications of adopting such measures

4.1 The technical measures in place

All of the teachers involved in the research (n=444) reported that their educational establishment had some form of technical safety measure in place (see table 4.1 below).

Table 4.1   Technical safety measures in place

Technical measure	Per cent
A Firewall	85
Local Education Authority provided filtering	80
Internet Service Provider filtering	73
Monitoring of pupils' accounts	62
A walled garden	15
In-house filtering	5
Supervised internet access	1.5
Other (e.g. anti-virus, fixed sites, no access)	5.5

The research found that systems were common and multiple, although there may have been some confusion amongst teachers as to who their filtering was provided by, hence the duplication of those reporting that they had LEA and Internet Service Provider filtering in place. Few educational establishments employ just one technical measure, for example, 85 per cent of teachers reported that a firewall is in place, and 80 per cent also reported that their local authority provides a filtering system. However, in the majority of cases where the LEA was the provider (45 per cent) the educational establishment was *required* to adopt the system, in a significant minority (40 per cent) it came preloaded

on equipment and in only a minority of cases (15 per cent) did the educational establishments decide to adopt the system. Most choice was exercised in relation to monitoring pupils' accounts, a measure which 87 per cent of educational establishments choose to adopt. Thus, where there are a range of measures currently in place, not all are actively adopted (chosen) by establishments.

4.2   The adequacy of the measures in place

The research sought to ascertain the measures in place and their perceived adequacy. Irrespective of the measure or how it came to be adopted, the majority of teachers (77 per cent or more) reported that their measures were adequate (see Table 4.2. below).

Table 4.2   Perceived adequacy of the technical safety measures in place

	Adequate	Inadequate
Firewall	77	15
Walled Garden	79	11
ISP filtering	77	15
LEA filtering	77	15
Monitoring of pupils' accounts	81	12

Interestingly, the measure perceived to be the most adequate is that chosen most frequently by teachers in educational establishments (the monitoring of pupils' accounts), whereas those where there was least choice (ISP provided filtering, LEA filtering and a firewall) are perceived as less adequate, albeit marginally so.

Previous research (Wishart et al's 2002 study) found that 42 per cent of teachers' reported that they monitored the websites visited by pupils: this may be subtly different to the monitoring of pupil's accounts as was asked in this research, but the 20 per cent increase in monitoring of pupil activities is perhaps a positive sign. However, supervision of pupils' using

the internet was highlighted by one teacher as a *non-technical* measure which was part of a broader school strategy:

"We have to be quite specific about when children can use the internet. We have a rule that they are not allowed to use them when a teacher is not present in the room, so at wet plays or during playtimes or anything like that. Children can't use the internet unless they are working under the direction of the class teacher…….We basically try to work within a whole school ethos whereby we develop trust and respect for each other and pupils know that they have a certain degree of responsibility when using the internet"

Urban Primary school

Thus, the context in which a measure is applied may be significant. Where it is seen as a free-standing technical solution then it may reduce the ability of teachers to develop a culture of appropriate use, so the research suggests that a combination of measures may be a more effective approach.

Respondents within educational establishments were asked how they feel about the technical safety measures they have in place, whether or not they provide adequate protection from a range of potential risks: protection against SPAM, inappropriate email content, and unsuitable web content. The research shows that current technical systems are more adequate as protection against SPAM and unsuitable web content and least adequate as protection against inappropriate email content (see Chart 4.1 below).

Chart 4.1   Adequacy of protection from specific risks
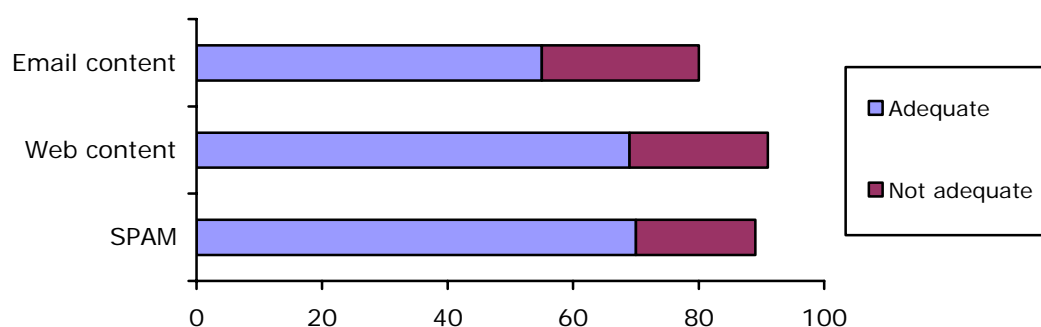
Thus, the adequacy of the technical safety measures in place varies by function. It is clear that there are some challenges around e-safety when a small, but significant minority of teachers report that they cannot offer adequate protection.

4.3 Staff use of the technical measures

The technical measures in place were easily or very easily understood by 39 per cent of teachers but 27 per cent did not understand them easily or at all and the remainder were uncertain. This suggests a degree of guidance or training may be required to enable teachers to use the technical measures more effectively.

The research examined where teachers went for support when encountering a problem with their technical measures, 49 per cent of teachers reported that they had to request help from the Network Manager, and 34 per cent reported that they had to request help external to their educational establishments. This lack of support within the establishment could be an inconvenience for a significant number of teachers.

4.4 Disruption of teaching and learning due to the technical measures

A key concern of this research was to examine the impact technical measures have upon teaching and learning. It is known that practice and routine can be disrupted by the technical measures in place and that subsequently teaching and learning may be compromised by the disruptions caused by the measures intended to protect children.

Teachers reported upon the frequency with which teaching and learning is disrupted as a result of the technical safety measures in place (see Table 4.3 below).

Table 4.3   Frequency of disruption to teaching and learning

Frequency of disruption	Per cent
Constantly (every day)	2
Frequently (two to three times each week)	7
Occasionally (at least once a month)	17
Rarely (less than once a month)	74

Few teachers reported constant, or even frequent disruption (two and seven per cent respectively), suggesting that it is a problem that affects few educational establishments. Most disruption was rare (74 per cent of cases) and this would indicate that the technical measures in place across educational establishments are not a major cause of disruption to teaching and learning.

There were no differences in terms of the frequency of disruption by school type. That is, teachers in Primary schools were no more or less disrupted than their colleagues in Secondary schools. Again, this points to difficulties that may be system specific – associated with the types of measures in place as opposed to the schools in which they are adopted. However, the research did find widespread variation in teachers' ability to adjust the measures in place. For example, only four per cent reported that they could adjust filtering levels according to their teaching needs. The majority (almost half) required help from within their educational establishments and a further 34 per cent required external support. This points to clear gaps in e-safety strategies across educational establishments. Although disruption caused by safety measures is marginal in most schools, teachers are not equipped to adapt measures to meet their needs (such as adjusting filtering to match their teaching needs).

4.4.1 Causes of technical problems

In order to try to identify the causes of disruption, educational establishments participating in Phase Two of the research were asked if they were able to equate disruption with a particular technical measure. It was clear that the majority of disruptions were caused by filtering (see Table 4.4 below).

Table 4.4   Sources of disruption to teaching and learning

Source of disruption	Per cent
Filtering set too high	44
Filtering set too low	13
Firewall restricted access to required sites	9
Filtering not working	7
Pupils overcoming security	4
Firewall not working	2
Other problem	31

Note: 'Other problems' includes broadband not working, hardware errors, upgrading server.

Filtering problems had two main features: being set too high *and* too low. This means that those teachers unable to adjust their filtering (the majority) face disruption at two levels: an inability to access some content; and the filter allowing access to inappropriate content. Where the filtering is set too low this may be the main concern of teachers (in terms of allowing access to inappropriate content), but there is a clear issue around the extent to which filtering systems are disrupting teaching and learning by preventing the appropriate use of ICT in classrooms. Allied to this is the evidence of firewalls restricting access and it could be that collectively, a degree of 'overprotection' and teachers' inability to adjust systems are posing problems in educational establishments.

Further statistical analysis of disruption caused by the technical systems in place was conducted. In order to see if firewalls were contributing to disruptions to teaching and learning the following hypothesis was designed and tested:

Testing research Hypothesis 4.1: Examining links between frequent disruptions to teaching and learning and educational establishments with a firewall

In order to examine the links between educational establishments that experience frequent disruption to teaching and learning and those establishments that have a firewall in place, a research hypothesis was designed and tested statistically.

Hypothesis 4.1:   Teachers reporting frequent disruption to teaching and learning will work in educational establishments where a firewall is *not* used.

Test: Spearman's Rho correlation

Result:	rs=-0.285; p=0.013 (p<0.05)
Summary:	As teachers reporting frequent disruption to teaching and learning are statistically more likely to work in educational establishments where a firewall is *not* used, the above hypothesis was accepted.
Comment:	Accepting hypothesis 4.1 suggests that the lack of a firewall is statistically linked to frequent disruption to teaching and learning. That is, having a firewall in place may protect teachers from disruption, whereas not having a firewall may increase disruption.

Statistically, teachers reporting disruption to teaching and learning are more likely to work in educational establishments where firewalls are *not* used. This suggests that the use of firewalls may *decrease* the likelihood of difficulties with the technical measures in place.

In summary, the main issues surrounding the technical measures and systems educational establishments have in place are that;

- some educational establishments have technical measures in place that they may not have chosen themselves
- teachers regard the monitoring of pupil accounts to be the most adequate of all measures they may have in place
- technical measures in place are least likely to protect children adequately from the content of emails
- a significant minority of teachers do not understand the technical measures educational establishments have in place easily, or at all
- disruption to teaching and learning as a result of the technical measures in place is rare
- few teachers reported that staff were able to adjust filtering easily according to their needs
- the most common cause of disruption to teaching and learning is due to inappropriate levels of filtering
- educational establishments with firewalls are less likely to encounter difficulties with their technical systems than those without.

4.5 The personal equipment allowed in schools

In Phase One of the research, teachers (n=444) were asked a range of questions about the kinds of technologies pupils used and the circumstances in which they were allowed to use them.

Teachers reported that they allowed the following equipment to be brought into their educational establishment by pupils:

- mobile phones (24 per cent)
- laptop computers (16 per cent)
- Personal Digital Assistants (PDAs) (13 per cent)
- other personal ICT equipment (13 per cent).

Teachers reported that they allowed pupils to use personal equipment in a range of circumstances (set out in Table 4.5 below).

Table 4.5   Circumstances in which pupils were permitted to use personal equipment

Circumstance of use	Per cent
When required for learning	13
During certain subjects only	10
Unsupervised	10
According to whether staff supervision is available	9
Contingent on signing the AUP	9
During lesson time only (but not subject specific)	8
According to their age	6
In the library	5
Before and after school only	3
For emergencies only (specifically mobile phones)	2
At break/lunch time	2
For SEN support purposes	1
Contingent on the situation	1

It is clear that the majority of circumstances in which pupils are allowed to use personal equipment is linked to teaching and learning, irrespective of whether use is subject specific. Supervision is also an issue, with some

pupils only allowed to use personal equipment under supervision. In fewer than ten per cent of educational establishments, use is contingent on signing the AUP, suggesting that AUPs are part of a wider strategy of use (as considered in Section Three).

In the majority of educational establishments (56 per cent), pupils were not allowed to use any personal equipment brought onto the premises for use on the establishments' computing equipment. In those cases where they were (46 per cent) they were allowed to use the following:

- CDs were allowed in 76 per cent
- floppy disks were allowed in 75 per cent
- portable devises, such as memory sticks, were allowed in 69 per cent
- software was allowed in 15 per cent of schools
- games were allowed in four per cent of schools.

This clearly has implications for e-safety, the transfer of information between settings and the risks pupils and others are exposed to in educational establishments. The links between breaches of e-safety and use of personal equipment will be examined in detail in Section Five; at this point it is sufficient to set out what is allowed and the context of its use in educational establishments.

Teachers were also asked about the kinds of new technologies pupils *were* allowed to use (for teaching and learning purposes) under supervision:

- use of web cams is allowed by 39 per cent
- use of Message boards is allowed by 21 per cent
- use of chat rooms is allowed by ten per cent
- use of mobile phone still photography is allowed by eight per cent
- use of mobile phone video photography is allowed by eight per cent
- use of web logs is allowed by seven per cent
- use of instant messaging is allowed by five per cent.

Once again the implications for e-safety are worthy of some consideration, specifically in relation to imagery and the circulation of such images, and

the potential for pupils to be exposed to potentially inappropriate persons online. Moreover, the risks may be considered to be age specific, with three times as many Secondary schools allowing web logs to be used than Primary schools.

However, further investigation during the telephone interviews with teachers in Phase Two suggests that the use of new technologies may be quite carefully monitored and linked to teaching and learning:

> *"We use DigiBlue video camera. We use them for all sorts of things – recording in PE, they're used for art projects, presentations, things like that, recording something the children have done".*

> Urban Primary school

Thus, permissiveness of new technologies and the use of pupils' own equipment need not increase risk.

In summary, the main issues surrounding personal equipment used in educational establishments are:

- the majority of teachers report that their educational establishment does not allow pupils to use any kinds of personal equipment on the premises
- of those educational establishments that do permit its use, most only allow such equipment to be used for specific teaching and learning purposes.

4.6 Technical Support provided by LEAs and RBCs

Research with LEAs (n = 25) and RBCs (n = 5) sought to examine the kinds of support they provided to educational establishments in relation to technical issues or systems.

The majority of LEA officers (88 per cent) and RBC officers reported that they *did* provide support to educational establishments regarding technical solutions:

- 70 per cent of LEAs provide technical solutions to educational establishments (compared to 75 per cent of RBCs)

- 78 per cent of LEAs offer assistance in maintaining systems (all RBCs do)

- 87 per cent of LEAs provide technical solutions to teachers (compared to 75 per cent of RBCs)

- 44 per cent of LEAs offer purchasing advice (compared to half of RBCs).

4.7 Summary of the section

The research examining technical measures and systems educational establishments have in place to protect pupils demonstrates a fairly wide variance in the difficulties experienced, and approaches taken by educational establishments. Educational establishments clearly perceive some measures to be more effective than others, although the research reports a significant lack of knowledge and understanding amongst teachers of the technical measures they have in place, and this may consequently have an impact on the degrees of disruption they encounter in their teaching and learning.

Educational establishments that consider some of the following approaches may experience an increased ability to manage the technical measures in place in their particular educational environment:

- setting aside some specific time for teaching staff to be informed about the basic ways in which the technical measures in the educational establishment operates, and how they can alter this for their own purposes

- looking into the possibility of installing a firewall on the system, or contacting the provider of their technical measures to discuss improvements to security

- regularly monitoring pupils' user accounts in order to further inform educational establishments of the efficacy of their systems.

The findings presented in this section suggest that educational establishments may need to be more pro-active in their employment and

administration of the measures they have in place, particularly exploring alternative ways to increase e-safety if they do not have the autonomy to choose their own technical measures.

5.0 E-safety challenges and approaches

A significant part of this study was to gauge the kinds of e-safety difficulties educational establishments are encountering: this was not by any means an attempt to criminalise educational establishments or provide sensationalist data, but to gain an understanding of what educational establishments encounter, and to consider the possible relationships between breaches of e-safety and other factors.

This section examines the kinds of breaches of e-safety that occur in educational establishments, the pupil groups that these breaches are prevalent amongst, and the actions educational establishments have taken in response to these breaches. Consequently, this section explores the kinds of educational approaches that teachers report their establishments are taking, and seeks to clarify areas of training that staff could benefit from.

5.1 Breaches of internet safety

Teachers participating in the research were asked to report upon the degree to which a range of breaches of e-safety were encountered in their educational establishment. These breaches were plagiarism, the intentional viewing of unsuitable online material, inappropriate use of mobile phones, bullying via mobile phones, bullying via chat rooms, websites or the World Wide Web, and attempts to breach educational establishments' security systems.

5.1.1 Plagiarism

It is generally held to be common knowledge that the World Wide Web is a plentiful provider of assistance to pupils with homework and coursework, but increasing concerns over the past few years of intentional plagiarism from websites, and the availability of essays and other works has meant that the issue has become one that all educators need to be aware of. In 2005, the QCA (Qualifications and Curriculum Authority) in a review of GCSE and GCE coursework acknowledged that the internet has increased the potential for plagiarism, and that further guidance was required for teachers in order to assist them in the identification of

plagiarism online. However, the issue of plagiarism is not confined solely to pupils' use of the World Wide Web; collusion between pupils in sharing or copying work is facilitated through the easy transfer of documents by email or data storage devices.

The majority of teachers (72 per cent) reported that their educational establishment did not encounter any plagiarism, although a significant minority, 12 and a half per cent, reported that their educational establishment had between one and five incidences of plagiarism in a typical month. Very small numbers of teachers reported that their educational establishments had difficulties with ten or more incidences of plagiarism per month.

In order to explore the possible reasons underlying increased incidences of plagiarism in some school and not others, a number of statistical tests were designed and implemented in order to consider the prevalence of plagiarism in schools in relation to other relevant factors:

Testing research Hypothesis 5.1: Examining the prevalence of incidents involving intentional plagiarism in relation to educational establishments that allow pupils to bring personal materials and items into school for use on school computing equipment

In order to examine the prevalence of incidents involving intentional plagiarism in educational establishments where pupils are allowed to bring personal materials and items into school for use on school computing equipment, in comparison to those where pupils are not, a research hypothesis was designed and tested statistically.

Hypothesis 5.1:	Incidents involving intentional plagiarism will be more prevalent in educational establishments where pupils are allowed to bring personal materials and items into school for use on school computing equipment than in educational establishments where they are not.
Test:	Mann Whitney test
Result:	$z= -7.199$; $p= 0.000$ ($p<0.01$)
Summary:	As incidents involving intentional plagiarism are statistically more prevalent in educational establishments where pupils are allowed to bring materials and items into school for use on school computing equipment than in educational establishments where this is not allowed, the above hypothesis was accepted.

Comment:	Accepting hypothesis 5.1 suggests that incidents involving intentional plagiarism will be more prevalent in educational establishments which permit pupils to bring materials and items into school for use on school computing equipment. That is, allowing personal equipment on site may increase the prevalence of intentional plagiarism.

Therefore the test suggests that plagiarism occurs more commonly in educational establishments that permit students to bring personal materials (such as CD's, memory sticks, games) onto the premises for use.

The data was interrogated further in order to ascertain if there were any further associations between educational establishments that allowed pupils to bring in personal equipment and the *frequency* of incidents of plagiarism, as shown below:

Testing research Hypothesis 5.2: Examining the frequency of incidents involving intentional plagiarism in relation to educational establishments that allow pupils to bring personal materials and items into school for use on school computing equipment

In order to examine the frequency of incidents involving intentional plagiarism in educational establishments where pupils are allowed to bring personal materials and items into school for use on school computing equipment, in comparison to those where pupils are not, a research hypothesis was designed and tested statistically.

Hypothesis 5.2:	Incidents involving intentional plagiarism will be more frequent in educational establishments where pupils are allowed to bring personal materials and items into school for use on school computing equipment than in educational establishments where they are not.
Test:	Mann Whitney test
Result:	z= -1.914; p= 0.056 (p<0.05)
Summary:	As incidents involving intentional plagiarism are not statistically more frequent in educational establishments where pupils are allowed to bring materials and items into school for use on school computing equipment than in educational establishments where this is not allowed, the above hypothesis was rejected.
Comment:	Rejecting hypothesis 5.2 suggests that incidents involving intentional plagiarism will be no more frequent in educational establishments which permit pupils to bring

> materials and items into school for use on school computing equipment. That is, allowing personal equipment on site may not increase the frequency intentional plagiarism.

The results of the test suggest that educational establishments that permit personal materials and items to be brought onto the premises for use on their computing facilities does not necessarily increase the frequency with which educational establishments may encounter incidences of intentional plagiarism.

Due to the increasing availability and use of memory sticks as a means to transport data, a similar test was carried out interrogating the prevalence of plagiarism in educational establishments that allowed pupils to bring in memory sticks onto the premises, as shown below:

Testing research Hypothesis 5.3: Examining the prevalence of incidents involving intentional plagiarism in relation to educational establishments that allow memory sticks on the premises

In order to examine the prevalence of incidents involving intentional plagiarism in educational establishments where pupils are allowed to bring memory sticks onto the premises, in comparison to those where pupils are not allowed to bring memory sticks onto the premises, a research hypothesis was designed and tested statistically.

Hypothesis 5.3: Incidents involving intentional plagiarism will be more prevalent in educational establishments where pupils are allowed to bring memory sticks onto the premises than in educational establishments where they are not.

Test: Mann Whitney test

Result: $z=-2.086$; $p=0.037$ ($p<0.05$)

Summary: As incidents involving intentional plagiarism are statistically more prevalent in educational establishments where pupils are allowed to bring memory sticks onto the premises than in educational establishments where they are not, the above hypothesis was accepted.

Comment: Accepting hypothesis 5.3 suggests that intentional plagiarism will be more prevalent in educational establishments that permit pupils to bring memory sticks onto the premises. That is, memory sticks may increase the prevalence of plagiarism.

The findings of the test suggest that educational establishments that permit memory sticks to be used on their premises may encounter more incidences of plagiarism than those that do not.

In summary, educational establishments may be less likely to encounter plagiarism if they reconsider their approaches to allowing pupils to use personal items, particularly memory sticks, on the premises, although of course, this would not preclude pupils copying from websites or their peers' work out of school. So once again, to tackle this issue will require more than an increase in rules or regulations, but strategies to increase pupils' awareness of the need to accurately identify any sources used in their work, and also to draw their attention to the potentially serious consequences of plagiarism, particularly with regard to coursework.

Teachers were asked about the prevalence of incidences of plagiarism according to year groups (see Chart 5.1 below).

Chart 5.1   Prevalence of plagiarism by year group
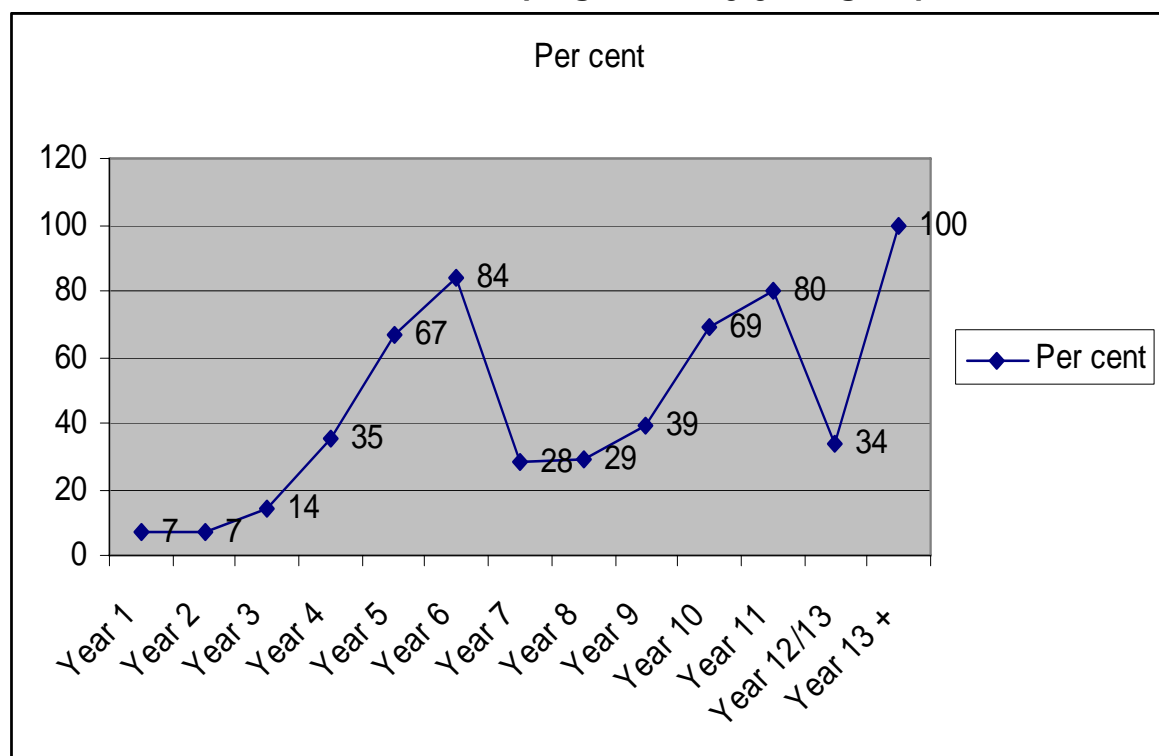
N.B   Year 1 – 6=   Primary schools, Special schools and PRUs
Year 7-12/13= Secondary schools, Special schools, PRUs
Year 12/13 -13+= FEs, PRUs and Special schools

Teachers reported that incidents of plagiarism were most common in the higher year groups of both stages of compulsory schooling, i.e. in years six, and in years ten and eleven.

In order to interrogate this finding further, a statistical test was designed and carried out, as shown below:

Testing research Hypothesis 5.4: Examining plagiarism from websites in Primary and Secondary schools

In order to examine incidents involving intentional plagiarism from websites by Primary school pupils compared to Secondary school pupils, a research hypothesis was designed and tested statistically.

Hypothesis 5.4:   Plagiarism from websites will be more common among Secondary school pupils than Primary school pupils.

Test: Mann Whitney test

Result: $z=-9.418$; $p=0.000$ ($p<0.01$)

Summary: As plagiarism is statistically more common among Secondary pupils than Primary pupils, the above hypothesis was accepted.

Comment: Accepting hypothesis 5.4 suggests that pupils at Secondary school are statistically more likely to be involved in plagiarism from websites.

The test showed that plagiarism (specifically from websites) was statistically more likely to occur amongst Secondary school pupils than Primary school pupils.

With regard to gender, just over half of teachers (51 per cent) reported that intentional plagiarism was common amongst both boys and girls, although a significant minority, 43 per cent, reported it was predominant amongst boys.

Teachers were asked about the kinds of consequences that pupils encountered as a result of being involved in incidences of plagiarism: the most common consequence was that pupils were punished within school, and that the pupils' parents were informed of the incident. Very few

teachers (three per cent) reported that pupils were asked to re-submit their work, and the same proportion reported that an exam board had been notified as a result of the plagiarism.

In summary, the research identified a number of factors that may make schools more prone to encountering incidents of plagiarism, namely with regard to the kinds of equipment pupils are allowed to bring onto the premises. Specific year groups were also found to be involved in incidents of plagiarism more than others. Educational establishments may be able to minimise and better manage incidents of plagiarism if they review their policies surrounding pupils' use of personal equipment on the premises, particularly for some year groups.

5.1.2. Intentional viewing of unsuitable material online

One of the principle concerns regarding children and young people's use of the internet has long been the risk that they will be exposed to inappropriate material online, such as content of an extreme sexual, racist, or violent nature. The research here focussed upon *intentional* viewing of online material, so as not to further identify inadequacies in technical measures, but to explore the prevalence of the problem from pupils actively seeking inappropriate content.

The majority of teachers (65 per cent) reported that they did not encounter any incidents of intentional viewing of unsuitable material online, although a significant minority (28.6 per cent) reported that they were aware of between one and five incidents in an average month.

In order to explore further any factors that might contribute to an increased prevalence of pupils intentionally viewing unsuitable online material, a statistical test was designed and tested with regard to educational establishments that permitted the use of personal equipment on their premises, as below:

Testing research Hypothesis 5.5: Examining the prevalence of the intentional viewing of unsuitable material online in relation to educational establishments that allow pupils to use personal equipment unsupervised

---

In order to examine the prevalence of the intentional viewing of unsuitable material online in educational establishments where pupils are allowed to use personal equipment unsupervised, a research hypothesis was designed and tested statistically.

Hypothesis 5.5: Incidents involving the intentional viewing of unsuitable material online will be more common in educational establishments where pupils are allowed to use personal equipment unsupervised than in educational establishments they are not.

Test: Mann Whitney test

Result: z=-7.502; p=0.000 (p<0.01)

Summary: As incidents involving the intentional viewing of unsuitable material online are statistically more prevalent in educational establishments where pupils are allowed to use personal equipment on the premises unsupervised where they are not, the above hypothesis was accepted.

Comment: Accepting hypothesis 5.5 suggests that the intentional viewing of unsuitable material online will be more prevalent in educational establishments that permit pupils to use personal equipment unsupervised. That is, allowing pupils to use personal equipment unsupervised may increase the prevalence of such activity.

The results from the test suggest that incidents involving the intentional viewing of inappropriate material online may be more prevalent in educational establishments that allow pupils to bring in personal equipment for use on the premises. This again has implications for educational establishments' policies in terms of the kinds of technologies pupils are permitted to use.

Teachers were asked to identify the year groups in which the intentional viewing of unsuitable online material was most prevalent amongst. As can be seen from Chart 5.2 below, incidences of the breach occurred most commonly in the older year groups within both school sectors (i.e. both primary and secondary).

Chart 5.2   **Prevalence of intentional viewing of unsuitable material online by year group**
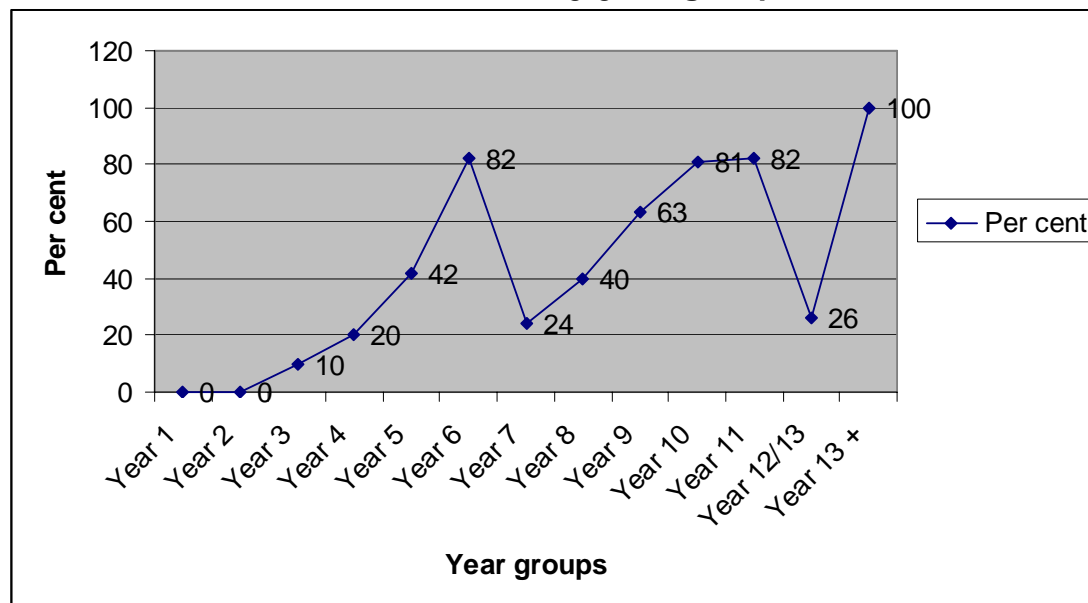
N.B   Year 1 – 6 =   Primary schools, Special schools and PRUs
        Year 7-12/13 = Secondary schools, Special schools, PRUs
        Year 12/13 -13+ = FEs, PRUs and Special schools

In order to explore the statistical significance of the ages at which the intentional viewing of unsuitable online material occurred, a statistical test was designed and carried out, as shown below;

Testing research Hypothesis 5.6: Examining incidents involving intentional viewing of unsuitable online material in Primary and Secondary schools

In order to examine incidents involving intentional viewing of unsuitable online material by Primary school pupils compared to Secondary school pupils, a research hypothesis was designed and tested statistically.

Hypothesis 5.6:   Incidents involving intentional viewing of unsuitable online material will be more common among Secondary school pupils than Primary school pupils.

Test: Mann Whitney test

Result: $z=-13.134$; $p=0.000$ ($p<0.01$)

Comment: As incidents involving intentional viewing of unsuitable online material are statistically more common among Secondary pupils than Primary pupils, the above hypothesis was accepted.

Summary:	Accepting hypothesis 5.6 suggests that incidents involving intentional viewing of unsuitable online material may occur predominantly amongst pupils in secondary school age groups.

Thus, incidents involving the intentional viewing of unsuitable material online are more likely to pose a challenge to staff in Secondary schools.

The research also clearly demonstrates a gender split amongst those seeking out unsuitable content online; 82 per cent of teachers reported that incidents predominantly occurred amongst boys.

As with incidents of plagiarism, teachers reported that pupils were most likely to be punished for incidents of intentional viewing of unsuitable material in their educational establishment, or that pupils' parents were informed. Amongst other actions reported by teachers, ten per cent reported that internet access was denied to the pupil, and six per cent reported that the police were involved. One per cent of teachers (n = 1) reported that a pupil had been excluded as a result of the breach.

In summary, the issue of pupils accessing inappropriate material is still a concern, and as with plagiarism, increased incidences of pupils' intentionally accessing inappropriate material were found in educational establishments where personal equipment was allowed onto the premises. Despite high levels of incidents reported by teachers amongst year group six in primary school, teachers in secondary schools were statistically more likely to encounter incidents of pupils viewing unsuitable material online, and as might be expected, most teachers reported that incidents were predominant amongst boys. It may be necessary for teachers responsible for pupils in the latter years of primary age to be alerted to the fact that pupils in this age group are more likely to actively seek inappropriate content: in turn this may have implications for those responsible for monitoring and adjusting filtering or firewall levels according to pupil group.

5.1.3 Inappropriate use of mobile phones

This section asked teachers about the inappropriate use of mobile phones, for example, texting or taking phone calls at inappropriate times. This section does not cover bullying by mobile phone: this is covered further on.

74 per cent of teachers reported that they did not encounter problems with pupils using mobile phones inappropriately. However, ten per cent of teachers reported that they were aware of between one and five incidents in an average month. Six per cent (n = 27) of teachers reported 21 or more incidents involving the inappropriate use of mobile phones in an average month.

As suggested by earlier findings, breaches of e-safety can occur more commonly in educational establishments that permit pupils to bring in various kinds of technological equipment onto the premises. In order to ascertain if this was the case in relation to the inappropriate use of mobile phones, a statistical test was designed and carried out to test this, as shown below:

Testing research Hypothesis 5.7: Examining the prevalence of the inappropriate use of mobile phones in relation to educational establishments that allow pupils to use personal equipment on the premises unsupervised

In order to examine the prevalence of the inappropriate use of mobile phones in educational establishments where pupils are allowed to use personal equipment on the premises unsupervised, a research hypothesis was designed and tested statistically.

Hypothesis 5.7:   Incidents involving inappropriate use of mobile phones will be more common in educational establishments where pupils are allowed to use personal equipment on the premise unsupervised than in educational establishments where they are not.

Test: Mann Whitney test

Result: z=-9.068; p=0.000 (p<0.01)

Summary: As incidents involving inappropriate use of mobile phones are statistically more common in educational establishments where pupils are allowed to use personal equipment on the

premise unsupervised than in educational establishments where they are not, the above hypothesis was accepted.

Comment: Accepting hypothesis 5.7 suggests that incidents involving inappropriate use of mobile phones will be more prevalent in educational establishments that permit pupils to use personal equipment on the premise unsupervised. That is allowing pupils to use personal equipment unsupervised may increase the prevalence of inappropriate mobile phone use.

The results of the test suggest that educational establishments that allow personal equipment to be bought onto the premises may encounter more incidents involving the inappropriate use of mobile phones than those that do not.

The age groups in which incidents involving the inappropriate use of mobile phones occurred was examined and teachers again reported a predominance of incidents in the upper years of both Primary and Secondary schools, although the difference between Primary and Secondary school pupils was marked in this case, which is likely to be due to the increased ownership of mobile phones amongst older pupils (see Chart 5.3).

Chart 5.3   **Prevalence of inappropriate use of mobile phones by year group**
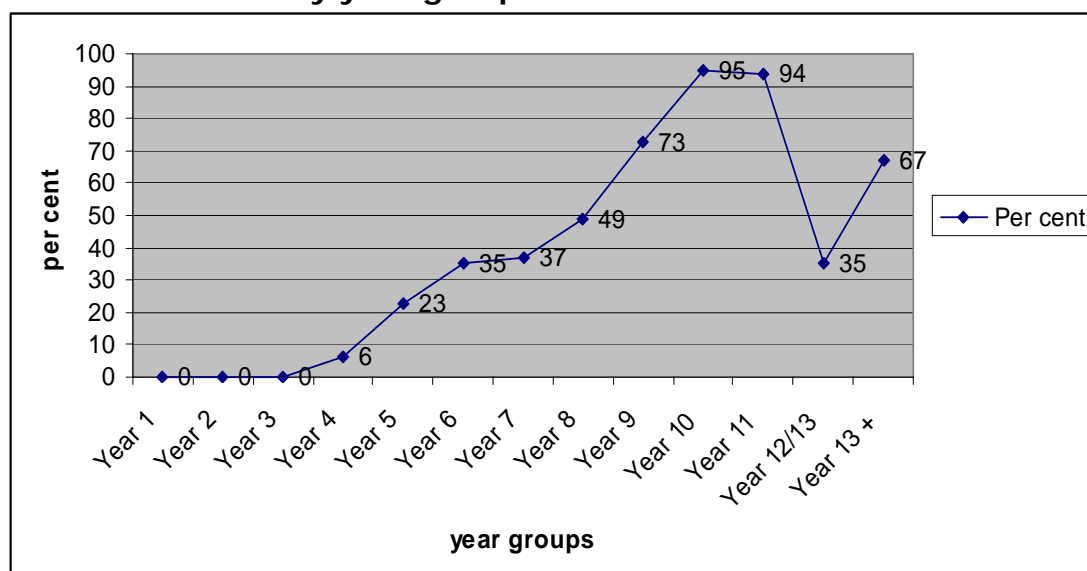
N.B   Year 1 – 6=   Primary schools, Special schools and PRUs
       Year 7-12/13= Secondary schools, Special schools, PRUs
       Year 12/13 -13+= FEs, PRUs and Special schools

The high number of incidences occurring amongst Secondary school pupils (particularly years ten and eleven) was examined by a statistical test, as shown below:

Testing research Hypothesis 5.8: Examining incidents involving the inappropriate use of mobile phones in Primary and Secondary schools

In order to examine incidents involving the inappropriate use of mobile phones by Primary school pupils compared to Secondary school pupils, a research hypothesis was designed and tested statistically.

Hypothesis 5.8:	Incidents involving the inappropriate use of mobile phones will be more common among Secondary school pupils than among Primary school pupils.
Test:	Mann Whitney test
Result:	$z=-15.948$; $p=0.000$ ($p<0.01$)
Summary:	As incidents involving the inappropriate use of mobile phones are statistically more common among Secondary school pupils than Primary pupils, the above hypothesis was accepted.
Comment:	Accepting hypothesis 5.8 suggests that mobile phones are used inappropriately by older pupils. Although Primary school pupils may use mobiles inappropriately, Secondary school pupils are statistically more likely to do so.

Most teachers (67 per cent) reported that the inappropriate use of mobile phones occurred equally amongst both boys and girls, although a significant minority, 23 per cent, reported that incidents occurred predominantly amongst girls.

With regard to action taken by educational establishments as a consequence of the inappropriate use of mobile phones, the majority of teachers reported that pupils were punished in school and that the incident was reported to the pupils' parents. 16 per cent of teachers reported that the pupils' mobile phone was confiscated.

One teacher involved in Phase Two of the research reported an incident involving the inappropriate use of mobile phones, which demonstrates the potentially serious nature of inappropriate use of them by pupils;

"When camera phones first came in…… the kids had gone round taking pictures of people around in the playground and they made this website up and got pictures from the school website of teachers and put it up on website and distorted them and put extra bodies on them……..they made themselves a site up on one of their parent's accounts…we got the police involved……and the parents as well because we had explained to the parents that because it had images of under 16-year olds on there and it was on their accounts – they could be on very dodgy ground"

Urban Secondary school

In summary, the prevalence of incidents involving the inappropriate use of mobile phones is affected by whether or not an educational establishment permits mobile phones onto their premises. As with other incidents reported in this section, pupils in Secondary schools are disproportionately likely to be involved in these kinds of incidents as opposed to Primary age pupils. This dilemma for educational establishments as to what kinds of equipment they might permit on their premises points to the need for exploration into the most appropriate ways of managing pupils' use of personal technologies within educational establishments' premises.

5.1.4 Bullying via mobile phones

Awareness of bullying via mobile phones has increased over the last few years, and children and young people have increasingly found ways in which they can absorb new technologies into bullying behaviour. Bullying via mobile phones may occur in a variety of ways, such as harassing phone calls, abusive or threatening text messages, and increasingly, using images or videos of bullying incidents recorded on a mobile phone then circulated to others (so called 'happy slapping' incidents).

However, encouragingly, the majority of teachers participating in this research (87 per cent) reported that their educational establishments did not encounter any incidents of bullying via mobile phone in an average month. 11 per cent of teachers reported that they encountered between one and five incidents and very small proportions (less than one per cent)

that they encountered more than 11 incidents of bullying via mobile phone in an average month.

In light of earlier associations between breaches of e-safety and educational establishments that permit equipment onto their premises, a statistical test was designed to test the hypothesis that incidents of bullying via mobile phone would be more prevalent in educational establishments that permitted pupils to bring mobile phones onto the premises than those that did not, as shown below:

Testing research Hypothesis 5.9: Examining the prevalence of bullying via mobile phones in relation to educational establishments that allow mobile phones on the premises

In order to examine the prevalence of bullying via mobile phones in educational establishments where pupils are allowed to bring mobile phones onto the premises, in comparison to those where pupils are not allowed to bring mobile phones onto the premises, a research hypothesis was designed and tested statistically.

Hypothesis 5.9:	Bullying via mobile phones will be more prevalent in educational establishments where pupils are allowed to bring mobile phones onto the premises than in educational establishments where they are not.
Test:	Mann Whitney test
Result:	$z = -3.341$; $p = 0.001$ ($p < 0.01$)
Summary:	As bullying by mobile phone is statistically more prevalent in educational establishments where pupils are allowed to bring mobile phones onto the premises than in schools where they are not, the above hypothesis was accepted.
Comment:	Accepting hypothesis 5.9 suggests that bullying via mobile phones will be more prevalent in educational establishments that permit mobile phones on the premises.

The test suggested that bullying via mobile phone is more likely to occur in educational establishments that allow pupils to bring mobile phones onto the premises than those that do not. A similar test was conducted in order to establish whether incidents of bullying via mobile phones occurred more *frequently* in educational establishments that allowed pupils to bring their mobile phones onto the premises:

Testing research Hypothesis 5.10: Examining the frequency of bullying via mobile phones in relation to educational establishments that allow mobile phones on the premises

In order to examine the frequency of incidents involving bullying via mobiles phones in educational establishments where pupils are allowed to bring mobile phones onto the premises, in comparison to those where pupils they are not, a research hypothesis was designed and tested statistically.

Hypothesis 5.10:	There will be a greater frequency of incidents involving bullying by mobile phone in educational establishments where pupils are allowed to bring mobile phones onto the premises than in educational establishments where they are not.
Test:	Mann Whitney test
Result:	z=-2.518; p=0.012 (p<0.05)
Summary:	As there was a statistically higher frequency of incidents involving bullying by mobile phone in educational establishments where pupils are allowed to bring mobile phones onto the premises than in educational establishments where they are not, the above hypothesis was accepted.
Comment:	Accepting hypothesis 5.10 suggests that bullying via mobiles phones will be more frequent in educational establishments that permit pupils to bring mobile phones onto the premises.

Similarly, the test found that incidents occurred more frequently in educational establishments that allowed pupils to bring mobile phones onto the premises.

Teachers reported that incidents of bullying via mobile phones had occurred predominantly in the latter year groups of each school sector (as can be seen in Chart 5.4 below).

Chart 5.4   **Prevalence of bullying via mobile phones by year group**
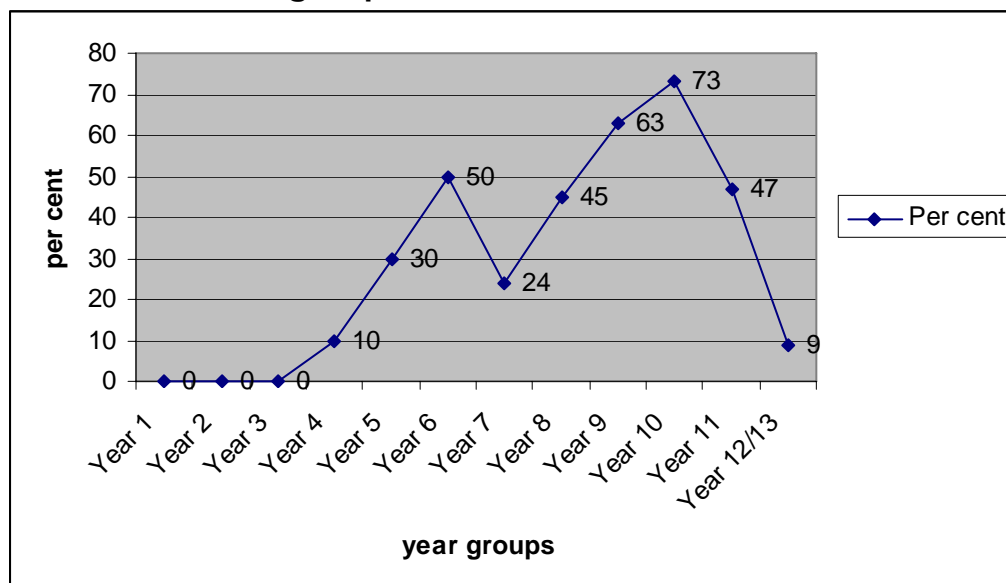
N.B   Year 1 – 6=   Primary schools, Special schools and PRUs
       Year 7-12/13= Secondary schools, Special schools, PRUs
       Year 12/13 -13+= FEs, PRUs and Special schools

In relation to gender, incidents involving bullying via mobile phones tended be slightly more common amongst girls, as reported by 47 per cent of teachers, although 31 per cent reported incidents were common to both gender, and 22 per cent that they were most common amongst boys, so although there is seemingly not as distinct a gender split evident in relation to this particular breach, a test devised and tested (below) showed that bullying by mobile phone is statistically more likely to occur amongst girls than boys.

Testing research Hypothesis 5.11: Examining incidents involving bullying via mobile phones in relation to gender

In order to examine incidents involving bullying via mobile phones in relation to gender, a research hypothesis was designed and tested statistically.

Hypothesis 5.11:   Incidents involving bullying via mobile phones will be more common among female pupils than male pupils.

Test: Mann Whitney test

Results: $z=-6.325$; $p=0.000$ ($p<0.01$)

Summary: As incidents involving bullying via mobile phones are more common among female pupils than male pupils, the above hypothesis was accepted.

Comment: Accepting hypothesis 5.11 suggests that girls are statistically more likely to bully other pupils using mobile phone technology than boys.

The findings of the test suggest that programmes of education or awareness-raising surrounding the issue of bullying via mobile phones may be more effective if tailored specifically towards girls.

As with other breaches, the majority of teachers reported that incidents were dealt with primarily within their educational establishments (reported by 90 per cent of teachers), and also that parents tended to be informed about the incident. Six per cent of teachers reported that their educational establishment had sought police involvement, which suggests that the incidents in question may have been of a fairly serious nature.

In summary, bullying by mobile phone is more likely to occur, and to occur more frequently, in educational establishments which permit pupils to bring their mobile phones onto the premises. A clear gender divide was found, with teachers reporting that incidents of bullying via mobile phone were more likely to occur amongst girls than boys.

5.1.5 Bullying via websites, chat rooms or email

Bullying via the internet can occur in a number of forms, such as persecution within a chat room or on message boards, threatening or nuisance emails, or even the setting up of hate websites which is a relatively rare phenomenon, but has occurred.

The incidents of bullying reported by teachers in this section are not differentiated according to the platform through which they took place (i.e. chat room, email or a website), but 15.5 per cent of teachers did report that they encountered between one and five such incidents in their educational establishment in an average month. However the majority of teachers (83 per cent) reported that they were not aware of the existence of any such incidents.

The research found that 81 per cent of teachers from educational establishments which taught within the Primary age range reported that incidents of bullying via new technologies (through websites, email or chat rooms) predominantly occurred amongst pupils in year six. All bullying incidents were less common among older pupils with the exception of year thirteen (see Chart 5.5 below).

Chart 5.5   Prevalence of bullying via websites, email or chat rooms by year group
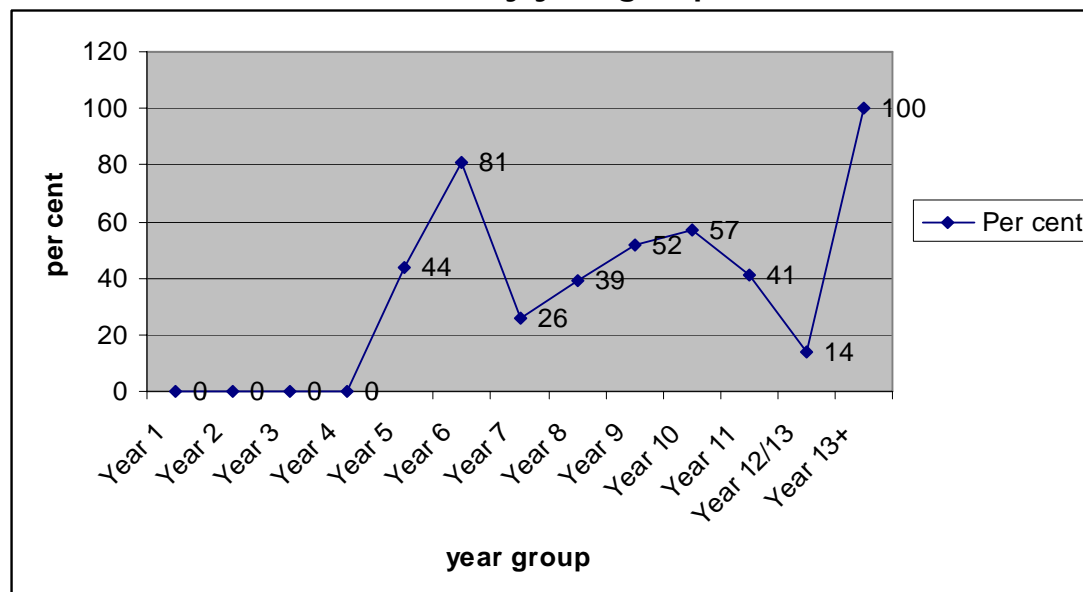
N.B   Year 1 – 6=   Primary schools, Special schools and PRUs
         Year 7-12/13= Secondary schools, Special schools, PRUs
         Year 12/13 -13+= FEs, PRUs and Special schools

Although a majority of teachers (47 per cent) reported that bullying via websites, email or chat rooms was equally common amongst both genders, 33 per cent reported that it was predominant amongst girls. In order to interrogate the statistical significance of these percentages, a hypothesis was designed and tested, as shown below:

Testing research Hypothesis 5.12: Examining incidents involving bullying via websites, chat rooms or email in relation to gender

In order to examine incidents involving bullying via websites, chat rooms or email in relation to gender, a research hypothesis was designed and tested statistically.

Hypothesis 5.12:   Incidents involving bullying via websites, chat rooms or email will be more common among female pupils than male pupils.

Test: Mann Whitney test

Results:	z=-6.083; p=0.000 (p<0.01)
Summary:	As incidents involving bullying via websites, chat rooms or email are statistically more common among female pupils than male pupils, the above hypothesis was accepted.
Comment:	Accepting hypothesis 5.12 suggests that bullying other pupils via websites, chat rooms or email is more common among girls than boys

In common with findings regarding bullying via mobile phones, this test suggests that girls are more likely to be involved in incidents of bullying via website, chat rooms or email than boys.

Again, teachers reported that the actions most commonly taken in relation to these kinds of incidents were punishing pupils within the educational environment, and also that the incident was reported to the pupils' parents. However, ten per cent of teachers did report that police involvement had been sought in relation to email, chat room or website bullying, which again suggests that some of these incidents were of a serious nature.

In summary, bullying via website, chat rooms or email is most likely to occur amongst girls, as were incidents of bullying by mobile phone. However, Primary age pupils in year six were more frequently reported by teachers as being involved in incidents of bullying online rather than by mobile phone, probably as a result of increased mobile phone ownership by pupils as they progress through school. The clear prevalence of bullying via ICT in general amongst female pupils suggests that more attention needs to be paid to particular groups of pupils in programmes of education not only about e-safety, but about bullying in general.

5.1.6 Contact involving potentially inappropriate persons

In tally with concerns over children viewing unsuitable material online, the issue of the internet and other communication technologies facilitating contact between minors and potentially inappropriate people (namely those with a sexual interest in children) underpins all concerns about children and young people's uses of information and communication

technologies. Thus, although a 'worst case scenario' incident, this issue is the most serious of all breaches explored within this research.

The vast majority of teachers (97 per cent) reported that they did not encounter any incidents involving contact with potentially inappropriate persons at their educational establishments. A small percentage of teachers (nearly three per cent) reported between one and five incidents involving contact with potentially inappropriate persons.

Although considering small numbers of pupils had been involved in such incidents, scrutiny of the age groups revealed that pupils in year six were most likely to have been involved in these incidents.

Chart 5.6 **Prevalence of incidents involving contact with potentially inappropriate persons by year group**
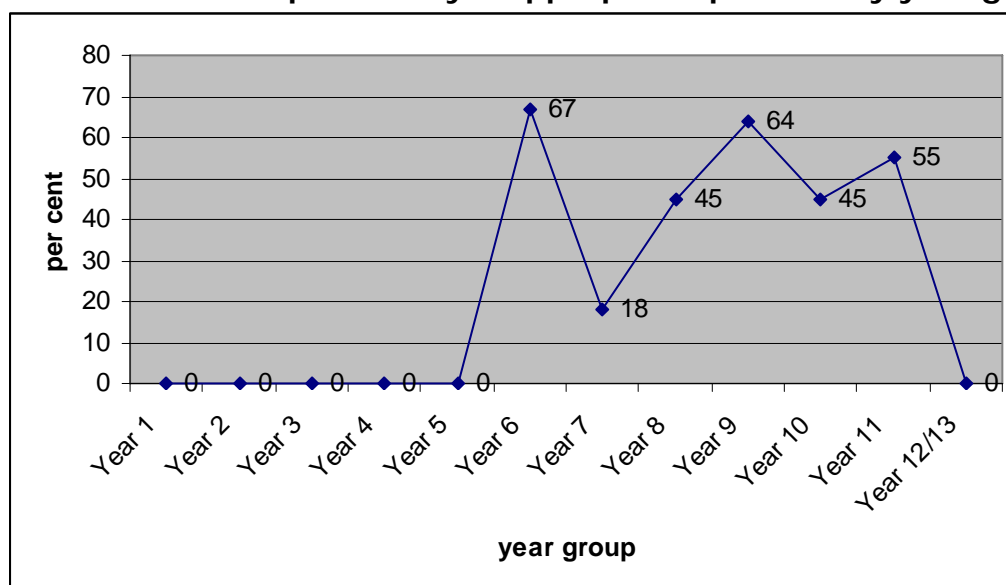
N.B   Year 1 – 6=   Primary schools, Special schools and PRUs
        Year 7-12/13= Secondary schools, Special schools, PRUs
        Year 12/13 -13+= FEs, PRUs and Special schools

As can be seen from the chart above, in contrast to other breaches where peaks of incidences at Secondary level tended to occur towards the end of pupils' school careers (in years ten or eleven), fairly high proportions of incidents are reported by teachers as occurring in earlier years, i.e. years eight and nine. This suggestion that contact with potentially inappropriate

persons is more likely to occur amongst pre-teen or young teenage pupils is in accordance with an emerging body of research which suggests that the most likely age at which young people may become involved with sexual offenders online is in their early teens (Finkelhor et al 2002:15, Carr 2004:3). Although this is a small body of research, it is validated to a degree by research examining the abuse of children *offline* which also places the most common ages for children to be targeted in their early teens (Gallagher et al 2002).

The research mentioned above also commonly finds that most incidents are perpetrated against girls, which was also reported by 64 per cent of teachers in this research. Therefore a hypothesis was designed and tested to see if this gender bias was statistically significant:

Testing research Hypothesis 5.13: Examining incidents involving contact with inappropriate persons (grooming) in relation to gender

In order to examine incidents involving contact with potentially inappropriate persons in relation to gender, a research hypothesis was designed and tested statistically.

Hypothesis 5.13:   Incidents involving contact with potentially inappropriate persons will be more common among female pupils than male pupils.

Test: Mann Whitney test

Result: z=-2.828; p=0.005 (p>0.05)

Summary: As incidents involving contact with potentially inappropriate persons are statistically more common among female pupils than male pupils, the above hypothesis was accepted.

Comment: Accepting hypothesis 5.13 suggests that that girls are at more risk than boys of contact with inappropriate persons and may require additional support.

The test supports trends identified in other research as it suggested that incidents involving contact with potentially inappropriate persons were more common amongst female pupils than male.

The research found that 38 per cent of teachers reported that pupils were punished in schools as a result of contact involving potentially inappropriate persons, although the nature of this punishment is unknown, so it is unclear as to whether this punishment was administered to rebuke pupils for taking actions to become involved with inappropriate persons, or whether the punishment was on a more preventative level. The study found that of those that had encountered an incident, five per cent of teachers reported that their educational establishment had sought advice from their LEA as a result of the incident, and the same proportion reported that they had sought advice from another (unidentified) source, whereas few teachers reported seeking guidance in relation to other e-safety breaches. 15 per cent of teachers also reported that the police had been involved as a result of the incident. Only 77 per cent of teachers reported that the incident had been reported to pupils' parents: this may be due to the individual nature of the incidents teachers were reporting, which was not revealed by this research, but common sense might expect this figure to be much higher due to the serious nature of the incident.

In summary, teachers reported that incidents involving contact with potentially inappropriate persons were rare, but where it had occurred, it occurred predominantly amongst girls, and those in year six, or in years nine, ten and eleven. These findings do not add any new information to the body of knowledge we have about the typical characteristics of children targeted online, but the fact that they are in line with what we already know confirms the reliability of these findings.

5.1.7 Attempts to breach school security systems

A concern with the use of all technologies in schools has always been regarding the potential for pupils to damage equipment or systems, and the high levels of knowledge and expertise amongst some young people about computer networks and the internet has meant that security systems can be a target for pupils.

Most teachers (71 per cent) reported that their educational establishment did not encounter any incidents involving attempts to breach the security system. However, 20 per cent reported that they encountered between one and five such incidents in an average month. Few teachers (four and a half per cent) reported more than ten such incidents in an average month.

As with other breaches of e-safety, any association between attempts to breach security systems and whether educational establishments allowed pupils to bring personal equipment onto the premises was explored to see if educational establishments were more likely to suffer attempts to breach their security systems if they did allow pupils to use personal equipment on the premises, as shown below:

Testing research Hypothesis 5.14: Examining the prevalence of attempts to breach e-safety security systems in relation to educational establishments that allow pupils to use personal equipment on the premise unsupervised

In order to examine the prevalence of attempts to breach e-safety security systems in educational establishments where pupils are allowed to use personal equipment on the premises unsupervised, a research hypothesis was designed and tested statistically.

Hypothesis 5.14:	Attempts to breach e-safety security systems will be more prevalent in educational establishments where pupils are allowed to use personal equipment on the premise unsupervised than in educational establishments where they are not.
Test:	Mann Whitney test
Results:	z=-8.559; p=0.000 (p<0.01)
Summary:	As attempts to attempts to breach e-safety security systems are statistically more prevalent in educational establishments where pupils are allowed to use personal equipment on the premises unsupervised than in educational establishments where they are not, the above hypothesis was accepted.
Comments:	Accepting hypothesis 5.14 suggests that attempts to breach the school security systems will be more prevalent in educational establishments that permit pupils to use personal equipment on the premises unsupervised. That is, allowing pupils to use personal equipment unsupervised may increase the prevalence of attempts to breach e-safety security systems.

As the test above demonstrates, incidents involving attempts to breach security systems are more prevalent in educational establishments that allow pupils to use personal equipment on the premises. Another test was carried out in order to see if educational establishments that allowed

pupils to use personal equipment on their premises encountered attempts to breach security systems more *frequently* than those that did not:

Testing research Hypothesis 5.15: Examining the frequency of attempts to breach e-safety security systems in relation to educational establishments that allow pupils to use personal equipment on the premise unsupervised

In order to examine the frequency of attempts to breach e-safety security systems in educational establishments where pupils are allowed to use personal equipment on the premises unsupervised, a research hypothesis was designed and tested statistically.

Hypothesis 5.15: Attempts to breach e-safety security systems will be more frequent in educational establishments where pupils are allowed to use personal equipment on the premise unsupervised than in educational establishments where they are not.

Test: Mann Whitney test

Results: z=4.292; p=0.000 (p<0.01)

Summary: As attempts to attempts to breach e-safety security systems are statistically more frequent in educational establishments where pupils are allowed to use personal equipment on the premises unsupervised than in educational establishments where they are not, the above hypothesis was accepted.

Comments: Accepting hypothesis 5.15 suggests that attempts to breach the school security systems will be more frequent in educational establishments that permit pupils to use personal equipment on the premises unsupervised. That is, allowing pupils to use personal equipment unsupervised may increase the frequency of attempts to breach e-safety security systems.

The test suggests that educational establishments which allow pupils to use personal equipment on their premises may be more likely to experience attempts to breach their security systems.

Examining the ages of pupils involved in attempts to breach security systems showed that teachers reported incidents occurring most commonly amongst pupils in years ten and eleven, although 70 per cent of teachers reported incidents occurring amongst children in year six, as can be seen in Chart 5.7 below.

Chart 5.7   Prevalence of attempts to breach school security systems by year group
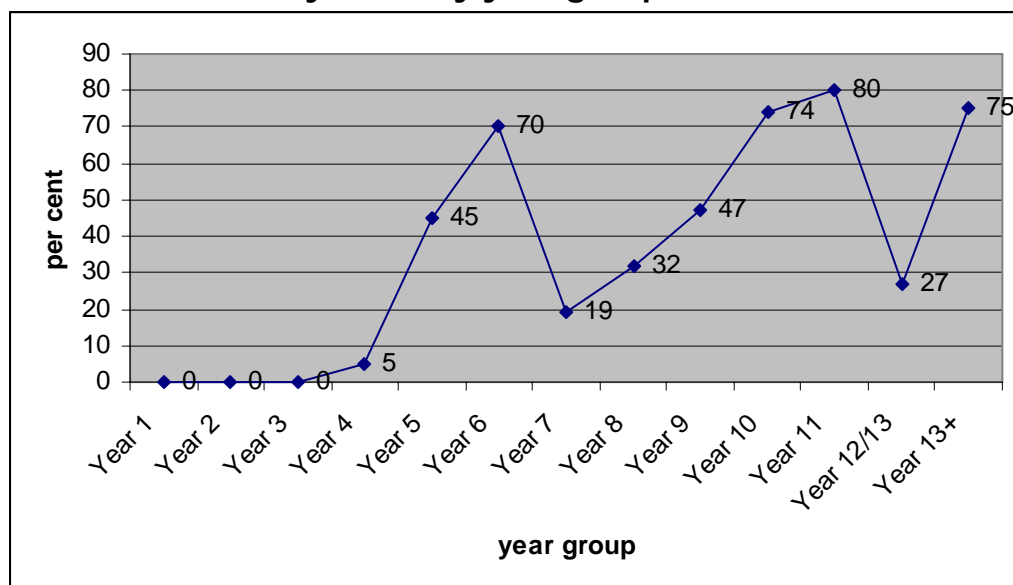
N.B   Year 1 – 6 =   Primary schools, Special schools and PRUs
        Year 7-12/13 = Secondary schools, Special schools, PRUs
        Year 12/13 -13+ = FEs, PRUs and Special schools

In order to validate the emerging theory from this research that breaches are more likely to occur amongst Secondary school pupils, a statistical test was developed and carried out in order to see whether this was the case in relation to attempts to breach school security systems, as shown below:

Testing research Hypothesis 5.16: Examining breaches of security systems in Primary and Secondary schools

In order to examine incidents involving attempts to breach the school's technical security systems by Primary school pupils compared to Secondary school pupils, a research hypothesis was designed and tested statistically.

Hypothesis 5.16:   Security breaches will be more common among Secondary school pupils than Primary school pupils.

Test: Mann Whitney test

Result: z=-15.368; p=0.000 (p<0.01)

Summary: As security breaches are statistically more common among Secondary pupils than Primary pupils, the above hypothesis was accepted.

Comment:	Accepting hypothesis 5.16 suggests that pupils at Secondary school are statistically more likely to breach technical security systems.

The test found that pupils of Secondary school age are more likely to be involved in attempts to breach security systems.

In terms of gender, 81 per cent of teachers reported that incidents involving attempts to breach security systems occurred predominantly amongst boys.

Out of all the breaches examined in this research, teachers were most likely to report that as a consequence of such an incident, pupils' parents were informed (93 per cent). A high proportion of teachers also reported that the incident was reported to their LEAS, possibly as a result of their filtering or other technical services being provided by them. Other actions taken as a response to incidents involving attempts to breach security systems included cancelling a pupils' internet access (11 per cent of teachers reported this).

In summary, both the prevalence and frequency of attempts to breach security systems are increased in establishments where pupils are permitted to bring personal equipment onto the premises. Incidents are reported as most commonly occurring amongst pupils (specifically boys) in year eleven, although high proportions of teachers also reported that incidents occurred amongst pupils in year six. Although within their respective educational environments, these are year groups that should be increasingly able to use technologies appropriately, the findings here suggest that closer monitoring of online activities and possible adaptation of technical security systems may be useful actions.

5.2 Guidance required by schools to counter e-safety incidents

In relation to the breaches of e-safety explored above, teachers participating in the research were asked about where they felt further advice about a range of possible breaches would be best directed at, i.e.

which groups of individuals required further guidance to counter that particular breach or issue of concern.

As can be seen from Table 5.1 below, teachers were more likely to report that pupils needed further guidance across all e-safety issues than other individuals.

Table 5.1   Incidents requiring further guidance

Incident	Pupils (per cent)	All teachers (per cent)	Governors (per cent)
Plagiarism	38	34	21
Viewing on online material	33	33	23
Inappropriate use of mobile phones	21	13	11
Bullying via mobile phone	25	22	19
Bullying via websites, chat rooms or email	29	28	22
Contact with potentially inappropriate persons	26	23	20
Breaching the school security systems	14	23	16
Average	28	25	19

Teachers were most likely to report that they felt pupils needed more guidance to counter the issue of plagiarism, and the viewing of unsuitable materials online than other breaches of e-safety. This may be because these are the issues that teachers encounter more frequently, or those which have a greater impact upon their teaching and learning practices. However, around a quarter of teachers (25 per cent and 29 per cent respectively) reported that they felt pupils needed to learn more to counter bullying via mobile phones, or by chat rooms, email or websites. These priorities were also reflected by teachers participating in the research who felt that other teachers in their educational establishment needed further guidance on these issues. Participants in the research also reported that they felt governors would benefit from receiving further guidance about e-safety issues, which suggests that in many educational establishments, governing bodies are regarded as important in relation to e-safety issues.

5.3 Recording of incidents

In order to consider the degree to which breaches of e-safety influenced educational establishments' policies and procedures, teachers were asked if their educational establishment kept a log of incidents. The study found that 59 per cent of teachers reported that their educational establishment did keep a log of incidents, but 34 per cent reported that their school did not and the remainder were unsure.

Teachers that reported their educational establishment did keep a log were asked about the range of details this log recorded. The majority reported that information recorded included the details of the incident, the date of the incident, the name of the pupil(s) involved, and the time at which the incident occurred. Only nine per cent reported that the action taken as a result of the incident was recorded, which may not facilitate the feeding back of information about past incidents into the development of future policies and practice.

LEAs and RBCs were also asked if they kept logs of e-safety incidents reported to them by educational establishment: 60 per cent of LEAs and 80 per cent of RBCs reported that they (either the respondent or another individual) did keep a log.

5.4 Measures schools have implemented to improve e-safety

An important part of this research is to build up a picture of not only the kinds of challenges educational establishments are facing with regard to e-safety, but particularly the kinds of actions they are taking to improve e-safety. The report has already presented a range of actions educational establishments are taking from a technical and policy perspective: this section's focus is more concerned with pedagogical approaches that are being implemented. Teachers reported taking a wide range of pro-active measures in order to improve e-safety within their educational environment, and this section looks at the nature and impact of including e-safety in the curriculum, the kinds of issues covered in such teaching, and the resources educational establishments are using to do this.

5.4.1 E-safety in the curriculum

Although the National Curriculum affords a number of opportunities to teach about e-safety issues, at present, e-safety is not a requisite, and the degree to which pupils are taught about e-safety varies considerably according to individual institutions. A key concern of this research was not to simply establish the proportion of teachers that reported their educational establishment taught about e-safety issues, but to consider the *impact* of these measures.

To this end, a statistical test was designed and implemented in order to assess the impact of including e-safety in the curriculum in relation to incidences of disruption to teaching and learning as a result of the establishments' technical systems, as is shown below:

Testing research Hypothesis 5.17: Examining the disruptions to teaching and learning caused by the technical systems in place and those educational establishments where pupils are taught about e-safety

In order to examine the disruptions to teaching and learning caused by the technical systems in place and those educational establishments where pupils are taught about e-safety, a research hypothesis was designed and tested statistically.

Hypothesis 5.17:   In educational establishments where pupils are taught about e-safety, teachers will report fewer disruptions to teaching and learning caused by the technical systems in place than where they are not.

Test: Mann Whitney test

Result: $z=-3.524$; $p=0.000$ ($p<0.01$)

Summary: As teachers are statistically more likely to report fewer disruptions to teaching and learning caused by the technical systems in place in educational establishments where pupils are taught about e-safety than in those where they are not, the above hypothesis was accepted.

Comment: Accepting hypothesis 5.17 suggests that educational establishment where pupils are taught about e-safety are likely to experience fewer disruptions to teaching and learning, caused by the technical systems in place. That is, teaching pupils about e-safety may reduce disruptions.

The results of the test suggest that educational establishments that teach pupils about e-safety may encounter fewer disruptions to teaching and learning. This may be due to the fact that pupils that have been taught about e-safety issues have a greater understanding of not only the risks they may encounter, but also the ways in which technical systems work to protect them.

Because the teaching of e-safety is not standardised in any way, pedagogical approaches taken vary, for both interventions aimed at pupils and staff, as can be seen in Table 5.2 below.

Table 5.2   Interventions aimed at teaching pupils and staff about e-safety

	Per cent
Embedded across other curriculum subjects	60
Teacher-led support offered to whole classes	57
Training other members of the teaching staff	42
Teacher-led support offered to individual pupils	36
Whole school activity	35
Training support staff	28
Used guidance from Becta	24
Parents' evening or event	12
Letters/leaflets sent to parents	5
Informal discussion with staff	1
Home/school agreement or policy	1
Other	1.6

Of those interventions most commonly cited, Secondary schools were more likely than Primary school to have implemented any of them, except for staff training, which was reported to occur more commonly in Primary schools. All teachers from Special schools reported that e-safety was embedded across curriculum subjects, in addition to whole school activities. Teachers from colleges of Further Education were less likely than other educational establishments to report that their institution implemented either whole school activities, or that e-safety was embedded across curricular subjects, probably due to the more fragmented and modular nature of teaching that many colleges employ. Small proportions of teachers from all kinds of educational institutions (Primary, Secondary, Special schools, Pupil Referral Units, or Colleges of

FE) reported that their establishment had implemented any kinds of activities aimed at parents or carers.

In Phase Two of the research, teachers were asked in which curricular subjects they taught about e-safety. Unsurprisingly, the most commonly cited curriculum area was ICT and PSHE, see Table 5.3 below.

Table 5.3   Subjects in which e-safety is taught

	Per cent
ICT	91
PSHE	41
History	30
English	28
Geography	23
Science	19
Other subject	19
Art	15
Religious Education	15
Maths	13
Modern Foreign Languages	11

5.4.2 E-safety issues pupils are taught about

As identified earlier in relation to some of the content of educational establishments' policies, new technologies, particularly those associated with mobile phones, were rarely covered, which may imply that some establishments have not yet begun to get to grips with the rapidly developing scope of technologies that children and young people favour. In order to explore this further, participants in Phase Two of the research were asked about the content that was covered when pupils in their educational establishment were taught about e-safety issues.

High proportions of teachers reported that pupils were taught about safe use of the World Wide Web and email (86 and 81 per cent respectively), although less reported that teaching covered the safe use of chat rooms (54 per cent). Fairly high proportions of teachers also reported that pupils

were taught about more complex themes relating to their use of the internet and other technologies, such as the reliability of information found online (68 per cent), how others might mask their identity (66 per cent), and recognising inappropriate conversations that might be initiated by some users (49 per cent). This finding is encouraging as these kinds of concepts are not necessarily context specific (i.e. they can be encountered in a range of situations using a number of different platforms) and so may be transferable to a range of situations. Lower proportions of teachers reported that children and young people were taught about newer, and particularly more recreational technologies that may not be permitted in educational establishments, i.e. bullying via mobile phones (41 per cent of teachers reported this), the safe use of mobile phones and peer to peer networks, (20 per cent respectively), and safe gaming online (17 per cent).

Another possible reason for the relatively low numbers of teachers reporting that their educational establishment taught about some issues could be as a result of the age groups they cater for. To this end, the data was interrogated further, where it was established that 71 per cent of Secondary school teachers had reported that their school taught about the safe use of email compared to 41 per cent of Primary schools. To determine the significance of this finding, a statistical test was carried out, as can be seen below:

Testing research Hypothesis 5.18: Examining the teaching of e-safety in Secondary schools, specifically the safe use of email, in relation to other educational establishments

In order to examine the teaching of e-safety education in Secondary schools, specifically the safe use of email in school, in relation to other educational establishments, a research hypothesis was designed and tested statistically.

Hypothesis 5.18: Teachers in Secondary schools will be more likely to have taught pupils about the safe use of email than teachers in other educational establishments.

Test: Mann Whitney test

Result: $z=-2.013$; $p=0.044$ ($p<0.05$)

Summary: As teachers in Secondary schools are statistically more likely to have taught pupils about the safe use of email in school than teachers in other educational establishments, the above hypothesis was accepted.

Comment:	Accepting hypothesis 5.18 suggests that Secondary school teachers may be more likely to teach their pupils about the safe use of email than teachers in other educational establishments.

The findings of the above test show that the likelihood of pupils being taught about the safe use of email increases with age, i.e. pupils are more likely to be taught about the safe use of email at Secondary school than at Primary. A similar test was carried out to see if this was also the case with regard to teaching pupils about the safe use of chat rooms, as 85 per cent of teachers in Secondary schools reported that their pupils were taught about this compared to 45 per cent of Primary schools. This test is shown below:

Testing research Hypothesis 5.19: Examining the teaching of e-safety in Secondary schools, specifically the safe use of chat rooms in school, in relation to other educational establishments

In order to examine the teaching of e-safety education in Secondary schools, specifically the safe use of chat rooms in school, in relation to other educational establishments, a research hypothesis was designed and tested statistically.

Hypothesis 5.19:	Teachers in Secondary schools will be more likely to have taught pupils about the safe use of chat rooms than teachers in other educational establishments.
Test:	Mann Whitney test
Result:	$z=-2.540$; $p=0.011$ ($p<0.05$)
Summary:	As teachers in Secondary schools are statistically more likely to have taught pupils about the safe use of chat rooms than teachers in other educational establishments, the above hypothesis was accepted.
Comment:	Accepting hypothesis 5.19 suggests that Secondary school teachers may be more likely to teach their pupils about the safe use of chat rooms than teachers in other educational establishments.

The test showed similar findings to the previous one, i.e. pupils at Secondary schools are more likely to be taught about the safe use of chat rooms than pupils of Primary school age. An integral part of the safe use of chat rooms regards inappropriate or unsuitable conversations that other users may attempt to initiate with children or young people, therefore a

statistical test was designed and implemented to see if the same age divisions existed as those for teaching pupils about the safe use of email and chat rooms:

Testing research Hypothesis 5.20: Examining the teaching of e-safety in Secondary schools, specifically about recognising inappropriate questions/conversations that may be raised by other users online, in relation to other educational establishments

In order to examine the teaching of e-safety education in Secondary schools, specifically about recognising inappropriate questions/conversations that may be raised by other users online, in relation to other educational establishments, a research hypothesis was designed and tested statistically.

Hypothesis 5.20: Teachers in Secondary schools will be more likely to have taught pupils about recognising inappropriate questions/conversations that may be raised by other users online than teachers in other educational establishments.

Test: Mann Whitney test

Result: z=-2.335; p=0.020 (p<0.05)

Summary: As teachers in Secondary schools are statistically more likely to have taught pupils about recognising inappropriate questions/conversations that may be raised by other users online than teachers in other educational establishments, the above hypothesis was accepted.

Comment: Accepting hypothesis 5.20 suggests that Secondary school teachers may be more likely to teach their pupils about recognising inappropriate questions/conversations that may be raised by other users online than teachers in other educational establishments.

The test above suggests that teachers tend to differentiate their teaching about the kinds of inappropriate conversations pupils may encounter in online situation, according to age. This further validates the overall finding from Phase Two of the research where 48 per cent of teachers reported that they differentiated e-safety teaching with regard to all issues according to the age of their pupils. However, entirely avoiding some issues in e-safety teaching may not be the most effective approach, as younger children are also using chat rooms and email (and increasingly, instant messenger programmes, as reported by Livingstone and Bober 2005), a more thematic approach which is not restricted to technological types or platforms, but according to risks or situations pupils may encounter in a range of contexts, might be preferable.

5.4.3 Resources schools use to teach pupils about e-safety

A range of resources intended to teach pupils about e-safety issues have emerged from a number of sources over the past few years, and these resources vary significantly in their approach and target audience. The majority of teachers that provided further detail about their pedagogical approaches to e-safety in Phase Two of the research (n=61) reported that they used resources developed within their educational establishment as opposed to resources provided by others, as demonstrated by several comments from teachers below:

"We developed our own curriculum resources for teaching PSHE and circle time lessons and things like that where we discuss particular things to do with internet safety"

Urban Primary school

"The LEA hasn't actually provided us with anything yet, it doesn't seem to be an issue for them at the moment so we've just taken it on our own initiative and the fact that it needs to be done, so we started investigating it ourselves and we're coming down the lines and finding things that are useful, and we're developing our own things………….when we were looking for resources we did a general scout everywhere and it's actually quite difficult to find some of these resources"

Urban secondary school

The study found that 60 per cent of teachers reported that they had used resources from the DfES or Becta's Internet Proficiency Scheme to teach pupils about e-safety. Also, 39 per cent of teachers said that their educational establishment had used resources from the LEA, 20 per cent had used ChildNet or Kidsmart, 18 per cent had used Becta's Signposts to Safety publication, 13 per cent had used the resources from the Home Office, and the same proportion reported using NCH. Few teachers (i.e. less than ten per cent) reported that their educational establishment had used resources from the Police, the BBC's ChatGuide, Save the Children and Think.com. Fairly small proportions of teachers reported that their educational establishment had held e-safety activities implemented by external bodies. Of those teachers whose educational establishment had used external bodies, one off activities provide by LEA advisors, volunteers, or the police were most commonly cited.

LEAs were asked about the kinds of support that they provided to educational establishments with regard to teaching about e-safety issues: 62 per cent of LEAs reported that they provided educational establishments with access to materials or resources to teach pupils about e-safety. These materials included Becta's Internet Proficiency scheme, posters, schemes of work, videos, and documentation, so it may be that some LEAs are signposting schools onto resources from other organisations.

5.4.4 Technologies used to teach pupils about e-safety

The ways in which educational establishments teach about e-safety was felt to be important, as the research has exposed a number of gaps in terms of new and recreational technologies that pupils may not be taught about. Few teachers reported that when teaching about e-safety, their educational establishment actually used the kinds of technologies they were teaching about; ten per cent of teachers reported that their school used message boards to teach pupils about e-safety issues, eight per cent that they used web cams, and three per cent that they used chat rooms. A combination of access to these technologies and the difficulties or risks that may be encountered when using these to teach in a 'live' context may be the reason behind low levels of use of these technologies. However, using these technologies as an integral part of teaching may benefit pupils firstly because visual aids can be more adept at demonstrating risks than narrative or abstract exercises, and also as pupils will have differing levels of access to technologies, so some may be able to relate what they are being taught to their experiences whereas others may have very little existing knowledge in which to contextualise the new information they are being taught.

5.4.5 E-safety training of school staff

In addition to exploring approaches used to teach pupils about e-safety, the research sought to establish the kinds of training that staff at various educational establishments may have received around e-safety.

Relatively low proportions of teachers participating in the research reported that staff (in a wide variety of roles) had received training around e-safety issues. Those staff most likely to have received training

included the ICT Co-ordinator, classroom teachers, the Head teacher, and the Child Protection Liaison Officer. Members of staff least likely to have received training were volunteers coming into the school, and classroom support staff, both of which are groups of staff that may be directly supervising pupils in their use of ICT, and so should be included in any training the school implements, although this may be difficult to arrange for some volunteers, particularly if there is a high turnover of them due to limited availability, placement rotations and so on. Most teachers (80 per cent) who reported that staff in their educational establishment had received training reported that it had been in the last 12 months.

Sources of training for staff varied, but the majority of teachers (67 per cent) reported that their training had been delivered by other members of staff, for example:

"We have trained about ¾ of them now – we've just had a big intake of staff and I haven't actually had chance to do their e-safety training yet, but the large majority of staff have had training on e-safety – what to look out for, what are the tell tale signs that there is an issue or that there is potentially going to be an issue. They are coping with that quite well"

Urban secondary school

The study found that 29 per cent of teachers reported that staff in their educational establishment had received training from their LEA, and 19 per cent from other sources such as INSET training. No teachers reported that their educational establishment had received training from the police or advisors/ consultants in the private sector. These findings again reflect fairly high levels of use of LEAs as a source of e-safety advice by educational establishments, and indeed just over half (57 per cent) of LEA officers participating in the research reported that they *had* provided e-safety training to educational establishments in their area, although evidence from interviews with teachers suggested that this LEA provision may not be sufficiently widespread yet;

"I think we need the LEA to make us more aware of the problems there are out there. We have a mature staff and some find it quite hard to get to grips with ICT. In a way people are bogged down with so many changes that have gone on in recent years. This is another thing they have to deal with – technology changes so much so quickly, I think staff lack confidence with a lot of things around ICT"

Urban Primary school

In addition to training supplied by some LEAs, all LEAs and RBCs reported that they provided educational establishments with background information about the risks associated with communication technologies. However, only two per cent of LEAs reported that they offer this as a matter of course, implying that educational establishments have to request this information specifically from the LEA (if they are aware that they can do so). The kind of issues that this information covers was explored and is shown in Table 5.4 below.

Table 5.4   Provision of information by LEAs and RBCs

Risks associated with...	Info provided by LEAs (n = 25)	Info provided by RBCs (n = 5)
Chat rooms	100%	100%
Instant Messaging programmes	89%	0%
Message boards	89%	100%
Web logs	44%	100%
Mobile phones	44%	0%
Video mobiles phones	33%	0%
Digital cameras	56%	50%
Portable equipment	38%	100%
Bullying via ICT	89%	50%
Viruses	100%	100%
Peer-to-peer networks	56%	100%
Other issues (e.g broadband)	0%	50%

The information provided by LEAs seems more up to date than that offered by educational establishment in that LEA officers report fairly high levels of advice offered about new and recreational technologies, although one teacher interviewed in Phase Two of the research reported that they would like more information to be provided:

"It needs to cover technical issues – as the kids are getting better, more and more people are getting computers at home – it's something that's quite important. I would love some external training, or even packs – I have nothing"

Urban Primary school

Advice LEAs and RBCs provided to teachers came from a range of sources: the most commonly cited was in-house expertise, despite the fact that as mentioned earlier, the majority of LEA and RBC staff (76 per cent) reported that they had not received any training relating to e-safety issues. The second most common source of advice used by LEAs and RBCs was Becta, then children's charities, other LEAs and the DfES.

One important factor that may influence the support and training offered by LEAs and RBCs to teachers could be levels of awareness amongst LEA and RBC staff. Some LEA and RBC staff *did* report that they were aware of a range of issues educational establishments were facing, such as the intentional viewing of unsuitable material, inappropriate use of mobile phones, bullying, and contact with potentially inappropriate people.

The kinds of provision LEAs and RBCs are offering can be assessed more effectively when the impact of the provision is considered. To this end, a key concern for LEAs and RBCs if they are providers of technical services may be the risk of pupils breaching security systems. In order to assess the impact of LEA and RBC advice upon teachers' capability to manage or reduce threats to their security systems, a statistical test was designed and implemented, as can be seen below:

Testing research Hypothesis 5.21: Examining teachers' need for support to counter threats to their school security systems in relation to that provided by their LEA

In order to examine teachers' need for support to counter threats to their school security systems and that provided by their LEA, a research hypothesis was designed and tested statistically.

Hypothesis 5.21: Teachers who express a need for further support to counter threats to their school security systems are less likely to feel appropriately supported by their LEA than those who do not need support.

Test: Mann Whitney test

Result: $z=-3.640$; $p=0.000$ ($p<0.01$)

Summary: As teachers who express a need for support to counter threats to their school security systems are statistically less likely to feel adequately supported by their LEA than those who do not, the above hypothesis was accepted.

> **Comment:** Accepting hypothesis 5.21 suggests that the advice provided by LEAs may be key to supporting teachers in countering threats to their school security system.

The test demonstrates that teachers who feel well supported by their LEA may be better placed to counter threats against their educational establishments' security systems, than those teachers who do not feel well supported by their LEA.

In summary, teachers reported a wide range of actions implemented in their educational establishment to improve e-safety, targeted at both pupils and staff, and in a small proportion of establishments, at parents.

5.5 Summary of this section

The research examining ways in which educational establishments take actions to improve their e-safety has highlighted key issues that both pupils and staff would benefit from learning more about. Crucially, clear associations have been established between the prevalence and frequency of various breaches of e-safety and schools that permit pupils to bring personal equipment onto the premises. The impact of teaching about e-safety has also been shown to have a direct impact on the prevalence of some breaches of e-safety.

However this section has revealed some gaps in the approaches taken by educational establishments *and* the support provided to them, which might be countered in a number of ways:

- Educational establishments (and LEAs that provide direction and support) must acknowledge the need to include issues associated with newer mobile and recreational technologies into their teaching about e-safety

- educational establishments might consider increased use of technologies where possible to teach about e-safety issues in order to ensure that all pupils can relate to and understand the safety messages they are being taught

- provision of training for staff needs to be reviewed, as at present the majority is delivered by other staff, or LEA staff, few of whom have received training themselves

- schools need to review the ways in which they manage pupils' use of and access to personal equipment that they bring onto the premises

- particular regard needs to be paid to some gender and age specific breaches of e-safety, which could be reduced through targeted initiatives at these groups of pupils.

Many of these recommendations will require a 'trial and error' approach according to individual educational establishments and pupil groups, and these kinds of experiences must be shared with other educational establishments and LEAs in order to promote good practice.

6.0 Future challenges and needs

The research findings presented in this report are of limited use if moves are not taken to consider how those responsible for supporting educational establishments in managing e-safety can best do so. One teacher participating in Phase Two of the research responded most positively to the prospect of developing technologies in schools by saying that,

" I don't actually think there are any challenges at all, I think it is just a case of informing them"

Urban secondary school

However, in order to ensure that all relevant members of the school communities *are* informed of any risks and subsequent action they should take, teachers participating in Phase Two of the research were asked about the *kinds* of resources and support that they felt would be useful to teach about e-safety in future. This section outlines possible ways forward in teaching about e-safety issues, taking into account some of the approaching challenges educational establishments face.

6.1 Resources needed to teach pupils about e-safety

There exist already a number of resources specifically designed to teach pupils about e-safety, such as Becta's Internet Proficiency Scheme and Signposts to Safety publication, Childnet's Kidsmart and KIA programmes, and a number of programmes originating in the U.S.A and Canada. However, such resources are still in their relative infancy, and so teachers participating in the research were asked about the kinds of resources they would like to have available to them to teach pupils about e-safety issues.

In terms of actual materials that could be used, most teachers reported that they felt teaching materials hosted online would be valuable, more so than those that felt hard copies of materials would be useful. This is interesting as earlier findings showed that few teachers reported using new technologies to teach about e-safety but are perhaps comfortable with use of the World Wide Web for sourcing information to be disseminated to pupils.

As can be seen from the table below, high proportions of teachers also believe that an interactive approach, involving games online or group activities would be valuable in teaching pupils about e-safety. Three quarters of teachers participating in the research believed that integrating e-safety into National Curriculum schemes of work would be valuable.

Table 6.1 Valuable resources for teaching pupils about e-safety issues

	Per cent
Teaching activities and materials available online	97
Games available online	92
Group games/activities	82
Experts coming into school to provide sessions	80
Games available on CD	77
Integration of e-safety issues into more National Curriculum schemes of work	75
Videos/DVDs	74
Teaching activities and materials available in hard copies	67
Leaflets for pupils	46
Books for pupils	44
Materials endorsed by age appropriate celebrities	32

It is also important that those developing such materials are aware of priorities according to teachers regarding the issues that such materials should cover. These issues and the percentage of teachers who felt that pupils should learn more about them are set out in the table below:

Table 6.2 E-safety issues that the pupils need to learn more about

	Per cent
How others may mask their identity online	87
Recognising inappropriate conversations that may be raised by other users	85
Safe use of mobile phones	85
Safe use of email	82
Provision of personal information to others via the internet	82
Safe use of the world wide web	80

Bullying via the web or mobile phones	78
Safe use of chat rooms	74
Safe use of gaming online	64
Plagiarism and reliability of information online	64
Safe use of peer-to-peer networks	62
Other issues	21

Note: 'Other issues' includes advertising pop-ups, technical issues and spy ware

Interestingly, the main area that teachers felt pupils should learn more about were those concerning contact with others, i.e. potentially inappropriate persons. This is however, not in accordance with earlier findings where only 26 per cent of educational establishments reported that they felt more pupils needed further guidance about this issue. Educational establishments may be unsure how to teach about this particularly sensitive and difficult area of e-safety, but do feel strongly that it should be covered.

Obviously, the issues presented here that teachers feel pupils should learn more about may depend upon a number of factors, such as the age of children, and also as highlighted earlier, the emphasis or approach within each issue may, and should, vary or be specifically targeted at pupils with regard to gender.

6.2 Resources needed to teach school staff about e-safety

As relatively low numbers of staff (particularly support staff) were reported to have received training around e-safety issues, teachers were asked what kinds of materials they thought would be useful to achieve this:

Table 6.3   Teaching school staff about e-safety

	Per cent
Experts coming into school to provide training	85
Documentation with background information about risks provided online	80
Documentation with background information about risks provided in hard copies	78
Leaflets	75
Other	32

Note: 'Other' includes videos/DVDs, activities, meeting with staff and parents, posters, visual games for SEN pupils, programme of study, regular updates from LEA, ,more time and training modules.

A high percentage (85 per cent) of teachers reported that they felt experts coming into their educational establishment to teach staff about e-safety issues would be valuable, and this feeling was reflected in the telephone interviews conducted with teachers in Phase Two of the research, as shown by this teachers' comment;

"An expert coming into the school to talk to the staff and maybe talk to the children in assembly. That would be great……..With the Every Child Matters document coming in, we should be aware of what the children are looking at, at home too – part of our duty of care is to ensure that they know what to do at home too"

Urban Primary school

Teachers were asked what kinds of issues they felt that other staff needed to learn more about, see Chart 6.4 below.

Table 6.4   E-safety issues that staff in educational establishments needed to learn more about

	Number	Per cent
Bullying via the web or mobile phones	45	75
How others may mask their identity online	43	72
Provision of personal information to others via the internet	41	68
Safe use of mobile phones	40	67
Safe use of peer-to-peer networks	40	67
Safe use of gaming online	38	63
Safe use of email	37	62
Safe use of chat rooms	37	62
Safe use of the world wide web	37	62
Plagiarism and reliability of information online	37	62
Other issues	17	28

Note: 'Other issues' includes viruses and security and pop up adverts.

Issues that staff may not be aware of were particularly emphasised by one teacher in Phase Two of the research,

"They need their understanding and awareness raised over issues and largely to do with things they [children] do at home because children don't bring mobile

phones into school but it is an issue that they need teaching around which might not come up at home about safe use of mobile phones"

Urban Primary school

Thus highlighting the dichotomy identified throughout much of this research, in that issues associated with technologies pupils are likely to use recreationally are frequently excluded from the scope of policies or e-safety teaching.

In summary, most teachers felt that the integration of e-safety into the National Curriculum would be a valuable way in which e-safety could be taught. Teachers felt that other staff would benefit from external organisations coming in to teach about e-safety issues. Both these suggestions have significant implications for school resources.

6.4 Future developments and their implications for e-safety in schools

The education system and a range of children's services and agencies face significant changes in their structure and scope over the coming years. Combined with this is of course the continuing evolution of technologies, thus the challenges faced by educators in relation to e-safety are not static, and will be influenced by a range of factors. Therefore the research asked teachers about two areas of change that would impact upon educational establishments, and also asked LEAs and RBCs about the impact of the developments in policy and provision for children at a local level.

6.4.1 Impact of extended schools on e-safety

A key government policy to secure quality care for children and to allow parents to work, is that of 'educare', whereby schools are intended to act as a central part of the provision for families within their communities, for example, through increased opening times and access to facilities and activities. Teachers were asked what impact developments such as these would have upon e-safety issues in their educational establishment. The majority of teachers (62 per cent), understandably, reported that they were uncertain about this, but 17 per cent felt that the trend of extended schools would have a 'very positive' or 'positive' impact, and 21 per cent

that it would have a 'negative' or 'very negative' impact. Thus teachers are generally unsure or concerned about the impact that extended schools will have on e-safety.

6.4.2 The impact of evolving technologies on e-safety

Naturally, the ever-increasing capabilities of technologies will have significant implications in educational establishments. The proportion of teachers reporting that these developments would have a positive impact were in the minority (21 per cent). Just under half of teachers (44 per cent) were unsure about the implications of technological developments, but 35 per cent felt developments would have a 'very negative' or 'negative' impact upon e-safety. These mixed feelings were reflected in Phase Two of the research where two teachers reported feeling positive, but wary of the rapidly changing landscape in which they and their pupils were operating;

"I think we're in a good position to take on anything new; we're certainly very receptive to improving our own use of ICT and improving the children's learning of ICT. When new technologies come into the domain of the school we're quick to take them on board and try to incorporate them into what we're doing"

Urban Primary school

…"it is still very much a new thing which the teachers and staff generally are still learning about and I think especially mobile technology is going to become a bigger part of education"

Urban secondary school

6.4.3 Future issues for LEAs and RBCS

The findings presented in this report suggest that many educational establishments are relying on their LEA (or in some cases their RBC) as a key source of guidance about e-safety issues. Recent legislation and changes in the landscape of provision for children on a local level will mean that increased consciousness of a range of issues, including children's safety online, will be required of LEAs and RBCs, however, only four per cent of LEAs and no RBCs reported that they had considered how issues relating to online child safety will be incorporated into arrangements to safeguard the welfare of children under section 11 of the Children's Act 2004.

6.5 Summary of this section

This section has highlighted a number of future challenges that educational establishments and other organisations should be aware of. Concerns over possible gaps in the content of information for pupils which have been identified throughout the research have been further confirmed by teachers reporting that children and young people need to know more about new technologies. However, as many teachers report that few members of their staff have received training in relation to e-safety, no amount of good intentions will ensure that teachers are actually *able* to teach about these issues. Future developments both technologically, and in terms of provision and support for educational establishments will pose challenges to a wide range of professionals, but as the research suggests a preference amongst educational establishments to use their LEA as a key source of information, it may be that the responsibility for e-safety needs to become one which local authorities adopt in a swift and pro-active manner.

7.0 Discussion of findings

This discussion seeks to explore some of the issues raised by the research in greater depth, and to provide grounding for the recommendations made at the beginning of this report. A number of salient issues arising from key research findings are explored in greater detail, and possible ways forward for educational establishments are considered. Several case studies are also included in order to provide contextual examples of how some of the good practice found by this research is implemented by educational establishments.

A key theme to emerge from this research is **the pressing need for educational establishments to adopt a firm and coherent approach** which is reflected throughout their strategic management in order to ensure that e-safety remains a high priority issue, and is taken into consideration in all other relevant areas of the institutions' policy and provision. For example, the research identified a number of factors that contributed to more effective management of e-safety within an educational establishment (as set out below). This must be encouraged by LEAs, who as a result of the Children Act 2004, have a duty to ensure that children using various services provided by the LEA and subsequently by educational establishments, are kept safe when doing so. The changing role of local authorities and the creation of Children's Services also strengthens the need for the issue of e-safety to become a responsibility at local level. This strategic support for **educational establishments** is required in order to ensure that they are able to take **a multifaceted approach to e-safety** in their particular educational environment. In-school strategies at a policy and procedural level identified by this research include:

- appointing a designated Internet or E-safety Co-ordinator

- communicating with the SMT in order to keep them informed of e-safety breaches, concerns or developments

- implementing an appropriate AUP which is sent home (possibly as part of a home-school agreement) and regularly revised

- the inclusion of e-safety in other school policies regarding child protection.

The case study below outlines how one **educational establishment** used two of these strategies as part of their approach to e-safety:

Case Study One: A proactive and forward thinking approach

Fairfields* is a large urban primary school in the Midlands, with clearly defined procedures and strategies to manage e-safety in the school. The school has a designated E-safety/ Internet Safety Co-ordinator, and the schools' Senior Management Team (SMT) is informed of e-safety issues on a regular basis through an established line of communication between the school's Network Manager and the Assistant head.

Generally, the school has few breaches of e-safety, although there have been a few incidences of inappropriate use of mobile phones and some viewing of unsuitable material – the school keeps a detailed log of these incidents.

Although the school feels that some of the staff are not overly confident with their use of technology, about three quarters of the staff have received training around e-safety issues, and the school generally feels that staff are coping well.

The school takes a proactive approach to their use of the World Wide Web in lessons – all staff are encouraged to test and check any sites they intend to use with classes prior to teaching, and any problems with new equipment or software are minimised through a rigorous testing regime prior to any new materials or resources being made available to pupils.

The school is keen on allowing pupils to bring in personal equipment when they need to for teaching and learning, for example, teachers have used mobile phones with video capabilities to record pupil projects, and the school will shortly be introducing a Virtual Learning Area, which will be used in classes to prevent some pupils feeling self conscious about asking for assistance from the teacher by raising their hand in front of their peers.

In terms of teaching about e-safety, the school offers support to individual pupils when needed, and e-safety is embedded across subjects in the curriculum, particularly in PSHE. The school has found it quite difficult to find resources to teach pupils about e-safety, and although they have drawn upon their LEA for support in general, they have not as yet been provided with any teaching resources, so they have been developing their own materials.

The school is forward thinking, with plans to teach pupils about peer-to-peer networks and online gaming, and they believe that mobile technologies are probably a development which has significant implications for them.

---

* All school names have been changed

The rapid development and expanding scope of technologies prompts challenges, not only in terms of the capabilities of technologies, but also with regards to the ways in which these are utilised by children and young people. This is particularly pertinent as the prices of, for example, internet enabled mobile phones fall and so become affordable to greater numbers of young people. One implication of this is that children and young people can exploit the opportunities these technologies afford.

A finding of particular interest regards the incidents of bullying by mobile phone or via websites, chat rooms and email highlighted by this research. It is hardly surprising that **children and young people have simply absorbed new technologies into their repertoires of routine behaviour, which for some young people, includes bullying**.

A number of research reports over the last few years have begun to recognise the emergence of this issue:

- In 2002, NCH reported that 16 per cent of children had been bullied by text, seven per cent through the Web, and four per cent by email

- In 2005, NCH conducted similar research again, and found that 20 per cent of children have experienced some form of digital bullying, and 14 per cent of children have experienced bullying via text message

- A joint survey by the NSPCC and the teen girls' magazine, Sugar[2], found that 13 per cent of girls admitted that *they* had sent intimidating text messages to others.

What is also worthy of consideration is the clear gender divide apparent in bullying incidents reported by teachers participating in this research. Teachers reported that incidents of bullying via mobile phone, or via email, chat rooms, and the World Wide Web, all occur predominantly amongst girls. There has long been interest in the apparent gender differences exhibited in bullying amongst children. Whitney and Smith (1993) assert that girls are more likely to be involved in verbal and psychological bullying than boys, and Sullivan et al (2003) cite Lloyd (1994) who argues that girls who bully tend to rely on a range of psychological weapons, such as persistent teasing, isolation from a group and the spreading of malicious rumours. All of **these behaviours that girls may be more likely to engage in are 'compatible'** (that is, they

---

[2] http://education.guardian.co.uk/pupilbehaviour/story/0,16806,1647460,00.html

can be carried out) **with technologies**. So, in one respect, technologies are simply another conduit through which children and young people can carry out existing behaviour. However, in another, it would seem that **technology has prompted, or enabled, a new kind of behaviour that we have observed over the past year, that of so called 'happy-slapping'**, where incidents of bullying (often physical abuse) are recorded via mobile phone video cameras and distributed. This enables potentially unlimited opportunities for the circulation and viewing of bullying incidents, thus increasing the harmful impact of the event. So, on the one hand technologies have become naturally absorbed into a bully's tools, and on the other, they have contributed to the creation of a new phenomenon, uniquely enabled through the capabilities of increasingly accessible technologies.

The challenge therefore, is for educators and others involved in this arena (such as charities and policy makers) to consider solutions which balance the risks with the advantages (such as those cited by Naismith et al, below): **it would be wrong to create a dichotomous environment between the home and school where technologies are the norm in one, and entirely banned in the other**, but educational establishments must try to ensure that they are safe environments for children and young people.

> *"Mobile technologies are becoming more embedded, ubiquitous and networked, with enhanced capabilities for rich social interactions, context awareness an internet connectivity…..Learning will move more and more outside of the classroom and into the learner's environments both real and virtual" (Naismith et al 2004:5)*

The most prudent way to determine which technologies are permitted in educational establishments, and in what contexts, will differ according to individual institutions, but the implementation of clear strategies that all pupils, parents and staff are aware of is essential. **Valid concerns of parents regarding the safety of their children moving to and from school cannot be compromised**, but the use of technologies, most obviously mobile phones, in school hours must be questioned, particularly in light of the association between bullying via mobile phones and

educational establishments that permit them onto their premises found by this research. This tension between the concern for children's welfare from parents and e-safety incidents in educational establishments highlights the need for parents to be kept informed of the educational establishments' e-safety concerns and policies, as the case study below demonstrates through it's use of AUPs and a clear policy of informing parents if their children are involved in any breaches of e-safety;

Case Study Two: Strategic involvement of the whole school community

The Oaks[3] is a small urban secondary school in the South West of England, which includes the whole school community in e-safety issues in an effective manner.

Crucially, the Senior Management Team and Governors are involved in e-safety issues if and when they occur in school, and they were also all involved in developing the AUP, which is revised annually in order to keep up to date. The AUP is used as a prominent tool in the school, as all teaching staff, parents, and pupils are required to sign it. The school also runs adult education courses, and all those who use the school's ICT facilities out of hours are required to sign the AUP too.

The school has had some difficulties with their technical measures (a firewall and Internet Service Provider provided filtering) disrupting teaching occasionally, and also the school is concerned that the technical measures do not really provide adequate protection from email content. There are few serious incidents involving ICT, although a fair degree of inappropriate use of mobile phones occurs. Pupils have also misused the Internet and email, but the school has a clear protocol regarding breaches, where the pupil is banned from using the network (for a fixed period of time) and a letter is sent home.

Their key concerns regarding e-safety are influenced by feelings that their ability to cope with e-safety is impacted upon by the limited financial resources the school has.

However, rules and regulations alone will not suffice: the research highlighted key ages (and gender differences) when incidents are most likely to occur: this suggests the need for both increased vigilance amongst teachers or network managers, and for targeted and tailored programmes of education which would address the needs of specific groups of young people.

---

[3] All school names have been changed

In order for the delivery of such programmes to be carried out effectively, the e-safety knowledge and skills of teachers must be brought under scrutiny. The research identified a number of factors that impacted upon teachers' ability to manage e-safety issues and incidents in their educational establishment, one such significant factor being the level of support received from their LEA. Consequently this means that **some pupils may be more vulnerable than others as a result of the levels of staff expertise in schools**. This clearly points to a need for training which covers e-safety issues to be embedded within both initial teacher training and continuing professional development: a move that has been called for by professionals in the internet safety arena for several years (NSPCC 2002[4]), and is consistently reiterated by Becta themselves (Becta 2005:16).

Although previous NOF training, which incorporated some elements of internet safety, has been subject to criticism, OFSTED identified a number of features of NOF training that *were* successful, which were: guidance that was tailored to meet individual needs, relevance to a teachers' subject, the provision of helpful feedback, and also high levels of support which tended to be present where training was supplied by smaller providers (OFSTED 2004:23). These are features that should be reflected in future e-safety training for teachers, particularly with regard to suppliers; possibilities regarding which organisations would be best placed to provide tailored training locally should be explored.

In terms of the actual content of training, findings from this research suggest that there may be **a gap with regard to new and emerging technologies in areas of educational establishments' policy and provision**: this gap can be closed if concerted efforts are made not only to provide training, but to ensure that it is regularly updated. One requirement for this will be that **an effective system of communication is used to inform teachers of up to date developments and risks** that they may encounter. A relatively low level of uptake of Becta's advice revealed in this study suggests that a dissemination route via LEA's (or Children's Services) may be more practicable.

---

[4] http://www.nspcc.org.uk/home/informationresources/teachertraining.htm

LEAs may be best placed as the key source of contact for schools with regard to other support and guidance, as educational establishments reported that they tended to use their LEA most frequently, as opposed to Becta or other sources. However, the research found evidence that support for educational establishments from LEAs was variable. In turn, LEAs themselves reported that they did not always have effective strategies in place to deal with e-safety issues, and that the majority of LEA staff responsible for issues of e-safety had received no training. Therefore, in determining the most effective means of keeping educational establishments informed about e-safety issues, whilst LEAs may be the most appropriate and familiar source of advice to teachers, there remain a number of significant shortcomings in their capability to do so.

Therefore the research findings present something of a dilemma for policy makers: should LEAs be designated contact points for educational establishments needing information and guidance about e-safety, or should efforts be concentrated upon increasing the visibility of Becta at a local level in order to encourage educational establishments to use Becta as a key resource? Both option carries with it implications of increased demand and consequently, these two key actors (Becta, and collective LEAs) must consider if they are sufficiently able and equipped to deal with a potential growth in need for their services. **For LEAs, extended responsibilities in this area would necessitate training for those individuals or teams responsible for e-safety**, and also an increased co-ordination and sharing of good practice *between* LEAs and RBCs. However, such decisions are likely to be influenced by, and to some extent dictated by, developments in the structure and scope of local authorities, meaning that such action may not be forthcoming in the near future. Therefore it is imperative that the issue of e-safety is incorporated into their future child protection agenda, and that it remains there.

Appendices

Appendix One - Methodological procedures used

Procedure Phase One

Initially 3 primary schools and one secondary school were sent questionnaires in 135 randomly selected LEAs. Following insufficient returns, the following procedures were followed in order to secure the sample;

Another random primary and secondary school was selected from each of the 135 LEAs

A further 2 primary schools and one secondary from each of the 135 LEAs were sent questionnaires

A third reserve sample of 956 Primary schools and 443 Secondary schools were identified. Nine Primary schools were drawn at random from those LEAs in which no Primary schools had returned a questionnaire, seven Primary schools were drawn from LEAs in which only one Primary school had returned a questionnaire and five Primary schools were drawn from LEAs in which only two Primary schools had returned a questionnaire. Five Secondary schools were drawn at random from LEAs in which no schools had returned a questionnaire

In summary, the initial school sample and subsequent reserve samples failed to secure sufficient returns until the final and significantly larger sample was drawn.

To obtain the Further Education (FE) College sample, a sample of 15 LEAs was drawn at random from a total of 150 LEAs, and one FE college was drawn at random from each LEA. Following insufficient returns, the following procedures were followed in order to secure the sample;

A second reserve sample of 30 colleges of FE was drawn at random from the LEA sample. Two FEs were drawn at random from each LEA.

Four of the 15 LEAs did not contain enough FEs to sample second reserves – three LEAs contained no more FEs and one LEA contained only one more FE. Therefore, an additional four LEAs were randomly sampled from the 150 LEAs.

Two FEs were drawn at random from three of the four additional LEAs and one FE was drawn at random from the fourth additional LEA. Therefore, the sample was drawn from 44 LEAs.

To obtain the Pupil Referral Unit sample, a sample of 15 Pupil Referral Units (PRUs) was drawn at random from a total of 447 identified

nationally. Following insufficient returns, the following procedures were followed in order to secure the sample;

A reserve sample of three PRUs was drawn at random from the same list.

Following insufficient returns, a second reserve sample of 30 PRUs was drawn at random from a total of 447 identified nationally

To obtain the Special school sample, a sample of ten Special Schools was drawn at random from a total of 1034 identified nationally. Following insufficient returns, the following procedures were followed in order to secure the sample;

A reserve sample of two Special schools was drawn at random from the same list.

Following insufficient returns, a second reserve sample of 20 Special schools was drawn at random from a total of 1034 identified nationally.

To obtain the Local Education Authority (LEA) sample, 52 English Local Education Authorities (LEAs) was drawn at random from a total of 150 LEAs. A reserve sample of five LEAs was drawn at random from the same sample.

All ten Regional Broadband Consortiums (RBCs) were included.

Procedure Phase Two

To obtain the Phase Two schools' sample, a sub-sample of 55 schools was drawn at random from the original Phase One sample (of 540 schools); 40 Primary schools and 15 Secondary schools. A reserve sample of five schools (four Primary and one Secondary) was drawn at random from the same sample.

Following insufficient returns from the schools identified for Phase Two, additional schools in the second reserve sample were notified (in a letter attached to their questionnaire) that they might be asked to take part in Phase Two and those returning a questionnaire were invited to take part until the target sample for Phase Two was reached.

A third step was taken when the sample was still incomplete; schools from the original sample and the 3rd reserve indicating that they would be happy to participate in further Becta research were randomly selected to make up the sample.

To obtain the Phase Two Further Education sample, a sub-sample of two colleges of Further Education (FE) were drawn at random from the colleges (of 15 FE colleges) that completed Phase One. A reserve sample of one college was drawn at random from the same sample.

As the two colleges identified from Phase one did not return a questionnaire, those that did (four colleges) were all invited to take part in Phase two and two colleges were available within the limited frame.

To obtain the Pupil Referral Units sample, a sample of two Pupil Referral Units (PRUs) was drawn at random from 15 PRUs completing Phase One. A reserve sample of one PRU was drawn at random from the same sample.

As two PRUs identified from Phase One did not return a questionnaire, those that did (eight PRUs) were all invited to take part in Phase Two but the relevant person from only two of the PRUs was available within the limited frame of the study.

To obtain the Special Schools sample, two special schools were drawn at random from those completing Phase One. A reserve sample of one special school was drawn at random from the same sample.

As the two special schools identified from Phase One did not return a questionnaire, those which did (six schools) were all invited to take part in Phase Two, but the relevant person from only two of the schools was available within the limited frame of the study.

Samples

Schools[5] Sample Phase one

	Number	Per cent
Primary school	303	68
Secondary school	123	28
Pupil referral unit	8	2
Special school	6	1
Further education	4	1
Total	444	100

---

[5] N.B: Unless specified otherwise, the term 'schools' when used in this report, will encompass primary schools, secondary schools, special schools, pupil referral units (PRU's), and colleges of further education (FE).

Of the individuals that completed the questionnaire, 60 per cent were female and 40 per cent were male.

Most of those who completed the questionnaire were the Head of ICT or the schools' ICT co-ordinator (N.B some respondents held multiple roles in school):

	Number	Per cent
Head of ICT/ICT Co-ordinator	345	78
Classroom Teacher	204	46
Assistant/Deputy Head	67	15
Head of Department	55	12
Network Manager	48	11
School Head/Principal	51	11
SENCO	22	5
Other	73	16

Schools' Sample Phase Two

A total of 61 educational establishments, including Primary schools, Secondary schools, Pupil referral units, Special schools and colleges of Further Education were involved in Phase Two of the research.

Type of educational establishment – Phase 2

	Number	*Per cent*
Primary school	42	69
Secondary school	13	22
Pupil referral unit	2	3
Special school	2	3
Further education	2	3
Total	61	100

LEA and RBC Sample

The sample was comprised of 25 LEAs and 5 RBCs

Respondents had a range of roles, such as Advisor for e-learning, Content and e-services manager, ICT advisor, ICT manager, technical consultant etc.

Appendix Two - References

Becta (2005) E-safety: Developing whole school policies to support effective practice Retrieved from
http://www.becta.org.uk/corporate/publications/documents/BEC5323_safety_DevWholeSchoolPoAW.pdf

Carr, J (2005) Child Abuse, Child Pornography, and the Internet NCH

Finkelhor, D, Mitchell, K and Wolak, J (2002) Online Victimization: A Report on the Nation's Youth u National Center for Missing and Exploited Children

Gallagher, B Bradford M an Pease, K (2002) 'The sexual abuse of children by strangers: its extent and nature, and victim's characteristics' in Children and Society Vol 16, part 5, pp346-359

Livingstone, S and Bober, M (2005) UK Children Go Online: Final report of key project findings LSE

Naismith, L Lonsdale, P Vavoula, G and Sharples, M (2004) Literature Review in Mobile Technologies and Learning NESTA Futurelab

NCH (2005) Putting U in the picture: Mobile bullying survey 2005 Retrieved from

http://www.nch.org.uk/uploads/documents/Mobile_bullying_%20report.pdf

Qualifications and Curriculum Authority (2005) A Review of GCE and GCSE coursework arrangements Retrieved from
http://www.qca.org.uk/downloads/qca-05-1845-coursework-report.pdf

Whitney, I and Smith, P.K (1993) 'A survey of the nature and extent of bullying in junior/ middle and secondary schools' in Educational Research 35 (1) pp3-25

Wishart, J., Dungworth, N and Smith, D (2002) Audit of Internet Safety Practices in English Schools: Final Report Retrieved from
http://www.becta.org.uk/page_documents/research/isafety_method_survey.pdf