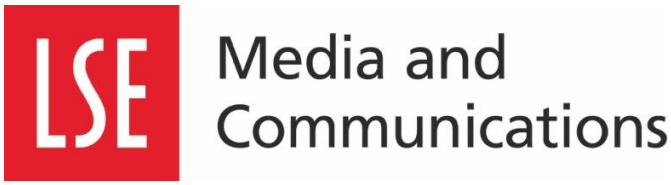
Children's online activities, risks and safety

A literature review by the UKCCIS Evidence Group

Professor Sonia Livingstone ▪ LSE
Professor Julia Davidson ▪ Middlesex University
Dr Joanne Bryce ▪ University of Central Lancashire
With Saqba Batool, Ciaran Haughton and Anulekha Nandi

October 2017



LSE Consulting
London School of Economics and Political Science

Houghton Street
London
WC2A 2AE
Tel: +44 (0)20 7955 7128
Fax: +44 (0)20 7955 7980
Email: lseenterprise.consulting@lse.ac.uk
Web: lse.ac.uk/consulting

Acknowledgements

This report draws on the expertise of the UKCCIS Evidence Group. We thank them for their input and feedback, and George Maier (LSE) and Emily Keaney (Ofcom) for working with us on the figures and tables included.

UK COUNCIL FOR CHILD INTERNET SAFETY

Contents

1. Executive summary

The UK Council for Child Internet Safety (UKCCIS) is a group of more than 200 organisations drawn from across government, industry, law, academia and charities that work in partnership to help keep children safe online.[1] The Council was established in 2008 following a review by Tanya Byron.[2] It deliberates and acts on topical issues concerning children's use of the internet.

Research findings are vital to provide the evidence base to inform stakeholder actions designed to improve children's online safety. Evidence can help estimate the scale and scope of problems, and provides an often necessary corrective to unfounded public anxieties, informing policy and practice. It can track changes in children's practices, informing the updating of advice, helping to frame and understand complex questions to which we lack common-sense answers – for example, about the nature of children's vulnerability in digital media. It is also important to know where gaps in the evidence base exist.

The UKCCIS Evidence Group identifies, evaluates and collates information from pertinent research findings, and communicates this to stakeholders with the aim of keeping UKCCIS, and the wider public, up to date. It holds seminars to address emerging issues, and produces a series of Research Highlights.[3] These provide succinct summaries of recent findings from UK-based research relevant to the UKCCIS remit, and currently number 108 in total.

In 2010 and again in 2012, the Evidence Group reviewed the available research, recognising that children's engagement with the internet and associated digital media continues to change, with new risks and safety issues arising and, fortunately, new research conducted to guide policy and practice. By early 2017 it was judged timely to review the available research afresh. Since the 2012 UKCCIS review (Livingstone et al., 2012a) the number of Research Highlights had doubled, and children's digital environment and modes of engagement, including the potential for risk of harm, are greatly transformed. In the wider policy field, the plan to develop an Internet Safety Strategy in 2017 makes an updated evidence review particularly necessary.[4]

A literature review identifies and synthesises findings and insights across multiple studies, bringing together the richness and depth of qualitative research reflecting children's own voices and experiences with the claims to national representativeness, longitudinal change over time and robust demographic comparisons that quantitative research makes possible. In this review, we stay close to the actual findings reported in recent studies, in order to capture empirical trends relevant to children's internet use, risks and safety in the UK. Thus we do not provide theoretical discussion, methodological debate or fuller contextualisation here.[5]

The scope of the present review was defined as research that:

- meets acceptable standards of quality[6]
- was conducted in or clearly relevant to the UK
- was conducted since 2012, with some exceptions where little subsequent research exists

[1] See www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

[2] See http://webarchive.nationalarchives.gov.uk/20101021152907/http://dcsf.gov.uk/byronreview/

[3] Available at www.saferinternet.org.uk/research

[4] See www.gov.uk/government/news/government-launches-major-new-drive-on-internet-safety

[5] See the detailed information and discussion in the sources cited in this review.

[6] For criteria, see www.saferinternet.org.uk/research/what-good-quality-research

- concerns children (0-17 years)
- concerns children's online activities, including the contexts and consequences of use.

In terms of methodology, the review draws on four sources: [7]

- the Research Highlights series and the research reports they summarise, focusing on those published since 2012
- a call for evidence circulated during February 2017 to UKCCIS members and other experts as well as via relevant mailing lists
- a keyword search of academic and grey literatures[8]
- research reports and publications already known to the authors.

In discussion with the Department for Digital, Culture, Media and Sport (DCMS), which commissioned this review, it was agreed that the review would address the following priorities, with an emphasis on:

- trends, to understand recent developments and anticipate emerging issues
- online risk of harm to children and implications for safety policy and practice
- key findings, linking to original reports, highlighting useful graphs and including verbatim quotes from children where available.

The key findings of this review are summarised below.

Children's internet access and use:

- While a small minority of children (mostly from poorer homes) remain without internet access, for most children, internet use is occupying ever more time, in more locations, including younger children (now four in ten 3- to 4-year-olds) and more personalised devices – although tablets are preferred over smartphones by younger children.
- Compared with other European countries, the UK is distinctive in favouring tablets over smartphones, and high levels of internet use in school.
- Motivations for using the internet vary mainly by age, and second by gender. Only a minority of children take up online opportunities for creative and civic participation, although many wish to be 'good digital citizens'.
- Risky opportunities vary – few children say they send photos to online contacts or reveal personal information, but a substantial minority uses services 'under age'.
- While it seems many UK children have learned to be cautious online, there is little evidence that their digital skills and literacies are increasing over time (although undoubtedly they increase with age).

Risk of harm online was the main focus of our review:

- Age is the key factor that differentiates among children's online experiences, with gender also significant.
- One in ten children to one in five young teens say they encountered something worrying or nasty online in the past year.

[7] This is not a comprehensive review; rather, we focus selectively on key evidence most relevant to UKCCIS' remit.

[8] We searched for [internet OR online OR digital OR 'mobile phone' OR app OR comput* OR 'cell phone' OR ICT OR 'social networking' OR platform OR broadband OR connect*] AND [child* OR young OR youth OR teenage* OR adolescent* OR minor OR kid OR girl OR boy OR student] AND UK.

- Children's top worries are pornography and violence; they say they encounter these most often on video-sharing sites, followed by other websites, then social networking sites and games.
- Children are also concerned about the levels of advertising online, their spending too much time online, inappropriate contacts, rumours and nastiness.
- Top parent concerns include online violence.
- There has been little increase or decrease in online risk in recent years, although there are some indications of a rise in hate and self-harm content.
- It is not possible to determine whether the internet has increased the overall amount of risk children face as they grow up, or whether the internet instead provides a new location for risk experiences, but the nature of the internet itself surely alters and amplifies the consequences.

In terms of *specific risks online*:

- Most research is on children's exposure to risk, with too little on which children come to harm and why, or what the long-term consequences are.
- Cyberbullying – estimates vary between 6-25%+ depending on measures – and the reasons for victimisation are diverse.
- Sexting and sexual harassment – most children experience neither; among those who do, such experiences are often associated with developing intimate relationships as teenagers.
- The wider context matters – the prevalence of gender inequalities, sexual stereotypes and coercion, and a lack of understanding of consent all serve to blur the boundaries between sexting and harassment; as a result, girls are more at risk, although there are also grounds for concern about boys.
- Online pornography – estimated prevalence varies, again by age and gender, but some estimates suggest the vast majority of teenagers have seen this; there is qualified evidence of adverse effects, including that children may be learning about sex from pornography, hence the importance of sex education.
- Sexual solicitation online – research suggests this may affect up to one in ten children; there have been some investigations of the behaviour of groomers, some of the consequences for victims, but there are many gaps here, and a need for a better understanding among child welfare professionals and criminal justice agencies.
- Radicalisation – there is a growing literature on this, but there are currently no UK studies related to online radicalisation of children.
- Some emerging research on children's involvement in hacking and cybercrime – through peer cultures inducing vulnerable youth or via online gaming, but this is recent and limited in scope.

Who is vulnerable or resilient?

- Consensus is emerging around the argument that those who can cope with a degree of online adversity, for whatever reason, may become digitally resilient, but those already at risk offline are more likely to be at risk and vulnerable online.
- There are correlations among risks so those children vulnerable to one type of risk are also likely to be vulnerable to others.
- There is some research on how vulnerable children face online risk, and on how resilient children cope – but more is needed here, especially in relation to long-term outcomes.
- A host of risk/vulnerability factors are likely to shape children's online experiences, and this is mediated by the ways in which children develop emotionally, cognitively, in terms of their identity needs, social relationships and need for support, and their peer cultures; however, it remains difficult except in retrospect to pinpoint the moment when children succumb to specific online risks.

Last, we reviewed the evidence for a *range of safety initiatives*:

- The overwhelming picture is that while diverse stakeholders have tried many initiatives, very few are independently evaluated. This makes it difficult to determine what works and why. Such evaluations as are undertaken tend to focus on immediate outcomes (reach, appeal, etc.) rather than a long-term reduction in harm or improvement in wellbeing.
- Schools use a range of strategies to implement e-safety priorities – including developing children's critical abilities – but there is mixed evidence of improvement, and such programmes tend to take a standard approach and may not be suited to the specific needs of more vulnerable children.
- Awareness-raising campaigns such as the Safer Internet Day have been instrumental in changing attitudes and practices.
- Parents use a range of mediation strategies including technical controls, rules regulating online access and use, including the majority preferring to talk to their children about the consequences of their online activities – but gaps remain in parents' abilities and skills for effective mediation; rules and restrictions tend to keep children safe but constrain their opportunities and invite evasion; enabling mediation is empowering providing children and parents have the skills and resilience to cope with risk when it occurs.
- Parents prefer to receive information about their children's online safety from schools despite information being available from multiple sources.
- Parents tend to prefer control tools they are familiar with unless an undesirable incident prompts them to adopt a new one.
- A range of industry initiatives exists in the form of agreements with the government, individual company policies and initiatives, and industry-level initiatives, but there is evidence to suggest that industry could do more to strengthen collaborative partnerships, particularly with law enforcement.
- Building children's digital resilience should have a twin focus on developing critical ability and technical competency in terms of education, as well as supporting children online and offline through constructive and informed parenting practices, through safety and privacy by design, and by improving the digital expertise of relevant welfare and other professionals who work with children.

2. Children's use of the internet

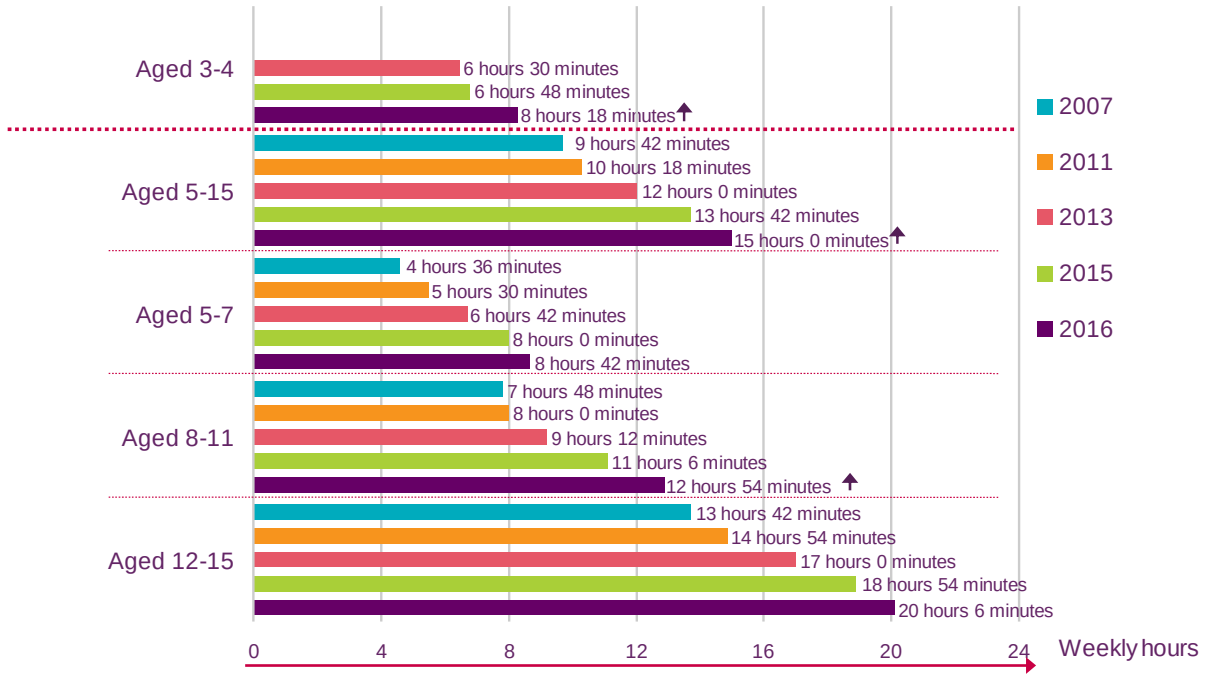
2.1 Main findings and trends over time

Children's use of the internet is changing fast, in response to considerable societal, market and technological innovation. Use depends in part on the children's gender, age and socioeconomic status (SES), and varies in the location, devices and frequency with which they access it.[9]

The 2012 UKCCIS Evidence Group's review noted that the amount (frequency, duration) of internet use had increased, including among younger children, over the previous years. By 2017, it appears that the proportion of children using the internet has reached a plateau: a recent survey by Childwise (2017) of 1,936 children aged 5-16 in Autumn 2016 found that 94% reported using the internet at all – 91% of 5- to 10-year-olds and 98% of 11- to 16-year-olds.

While the percentage of children using the internet has barely changed over the past five years, the amount of time they spend online continues to rise steadily. Ofcom's survey of 1,375 parents and children aged 5-15 using in-home interviews and 684 interviews with parents of children aged 3-4 (in Spring 2016) found that, among those who use the internet, weekly hours online have risen from over 9 hours in 2007 to around 15 hours for 5- to 15-year-olds in 2016, with even the 3- to 4-year-olds who go online doing so for some 8 hours per week (see Figure 1).

Figure 1: Estimated weekly hours of internet consumption by age, at home (2007, 2011, 2013) or elsewhere (2015 and 2016)



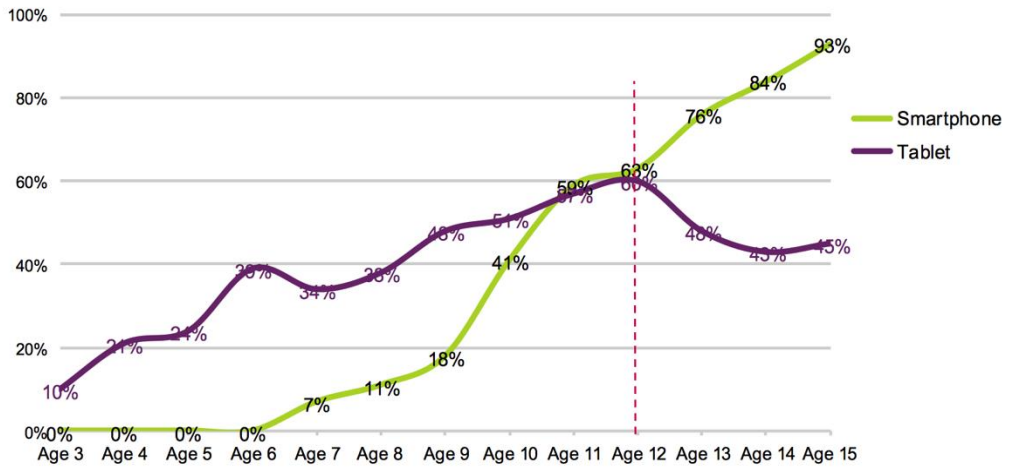
QP25A-B: How many hours would you say he/she spends going online on a typical school day/on a weekend day? (unprompted responses, single-coded) In 2007-12 the response for 12- to 15-year-olds was taken from the child and the parent for 5-7s and 8-11s. In 2007-13 (variable base) parents/children were asked about use at home whereas from 2014 they were asked about use at home or elsewhere.
Base: Parents of children aged 3-7 who use the internet at home or elsewhere and children aged 8-15 who use the internet at home or elsewhere. Significance testing shows any change between 2015 and 2016.
Source: Ofcom (2016a)

[9] Regarding children's access and use of the internet, we draw selectively on Ofcom's annual surveys; for further information see www.ofcom.org.uk/research-and-data/media-literacy

The device favoured to access the internet has also changed in recent years. By 2016 the rapid rise of the tablet made it the preferred device for younger children, with the smartphone still preferred among teenagers. Other devices for internet access are also used, but less commonly (Childwise, 2017; Ofcom, 2016a; WISEKIDS, 2014).

It seems that the tablet has become a key device for both personal and shared entertainment at home among younger children, but when children move from primary to secondary school, gaining their own smartphone becomes a priority (see Figure 2).

Figure 2: Tablet and smartphone ownership, by age



QPE3/F/QP4: I'm going to read out a list of different types of equipment that you may or may not have in your home, and which your child may or may not use (prompted responses, single-coded). You mentioned that your child has their own mobile phone. Is this a smartphone? A smartphone is a phone on which you can easily access emails, download apps/applications and other files, as well as view websites and generally surf the internet/ go online. Popular brands of smartphone include iPhone, Blackberry and Android phones such as the Samsung Galaxy (unprompted responses, single-coded).
Base: Parents of children aged 3-4 or 5-15 (396 aged 3, 288 aged 4, 157 aged 5, 140 aged 6, 101 aged 7, 181 aged 8, 129 aged 9, 92 aged 10, 101 aged 11, 143 aged 12, 108 aged 13, 105 aged 14, 118 aged 15).
Source: Ofcom (2016a)

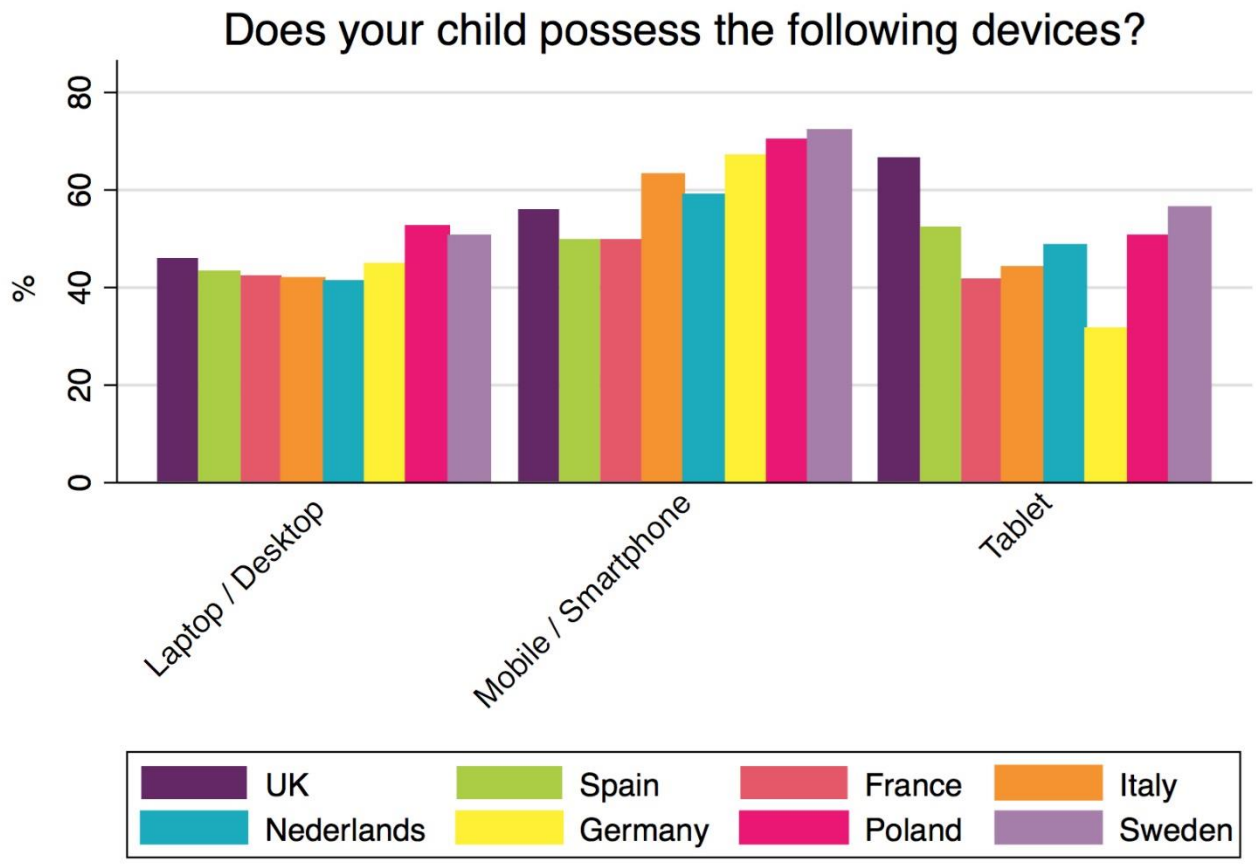
The appeal of multifunctional, mobile devices is strong, as demonstrated by this quote taken from WISEKIDS (2014):

> "My iPhone ... you can do everything with it. It's like an iPod, you can phone people, text people ... so Facebook, Snapchat, the Google app, the weather app ... just to see if it snows, YouTube ... free music, BBC iPlayer ... rugby football games.... Kik, BBM, Instagram." (Boy, 13-14 years old)

Findings for the UK can be compared with selected other European countries. A recent European Commission-funded project surveyed 6,400 parents of 6- to 14-year-olds, 800 in each of eight countries (Lupiáñez-Villanueva et al., 2016)[10] (see Figure 3 below).

This shows that UK children are more likely to possess their own personal tablet than in the other countries, but less likely to own a mobile or smartphone. This may reflect a cultural preference, or it may be that the UK is 'ahead' of Europe in a trend away from phones to tablets, particularly among younger children.[11] The safety implications of this trend are thought-provoking: perhaps it can be said that, especially for younger children, the tablet is safer both by operating largely on home Wi-Fi (which can be filtered) and being easier than the phone for parents to supervise.

Figure 3: Children's personal ownership of devices, by country



Q5: Does your child possess the following devices for her/his exclusive personal use?
Base: *N*=6,400 parents of 6- to 14-year-olds who use the internet, 800 in each country.
Source: Lupiáñez-Villanueva et al. (2016)

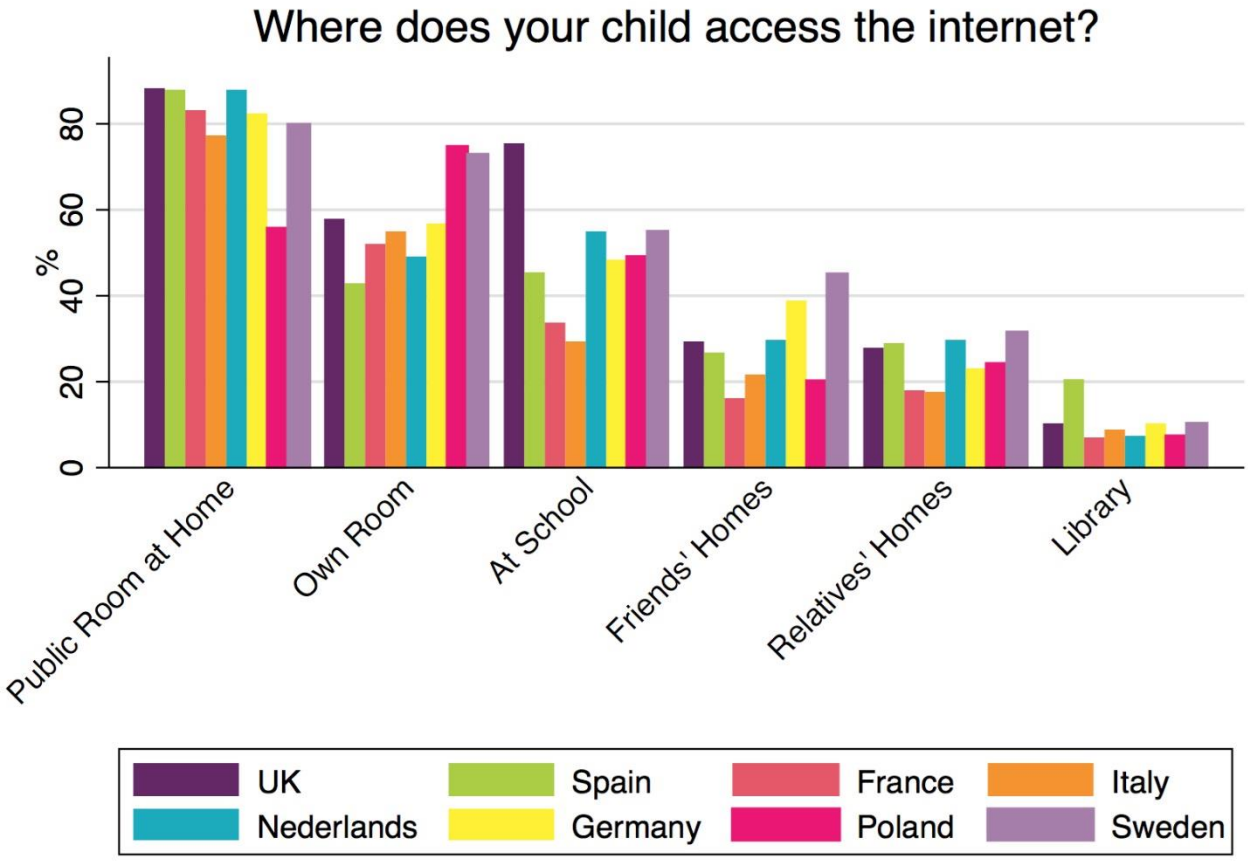
[10] This study was funded under the Request for Specific Services No. EAHC/FWC/201385 08 for the implementation of the Framework contract no. EAHC/2011/CP/01/LSE for the provision of a 'Study on the impact of marketing through social media, online games and mobile applications on children's behaviour'. It was produced under the Consumer Programme (2007-13) through a contract with the Consumer, Health, Agriculture and Food Executive Agency (CHAFEA), acting on behalf of the European Commission. See http://ec.europa.eu/consumers/consumer_evidence/behavioural_research/impact_media_marketing_study/index_en.htm

[11] As Ofcom (2016a, p. 22) notes of UK children, 'for tablets, increased access for 3-4s and 8-11s has not caused a corresponding uplift in use.'

The same survey also asked parents where their children use the internet (see Figure 4 below). Bearing in mind that this is data from parents, who may not know where their children use the internet at all times, the European comparison is again instructive:

- For UK children, a public room at home, followed by school, are the main locations of use. Other locations are not much used: while it is likely that smartphone users go online wherever they are, many children are constrained by cost and therefore tend to rely on access to home Wi-Fi.
- Research over the past two decades has consistently shown that more children in the UK use the internet than in other European countries, making school an important place for reaching children to teach digital and media literacy, including internet safety.
- The balance of use in public and private rooms has shifted over the years, and the high use of personal devices in public rooms may reflect both changing norms within the family and also parental efforts to ensure that their child's internet use can be monitored.

Figure 4: Children's internet access, by location and country



Q3: As far as you are aware, where does your child access the internet? By 'the internet' we mean going online on any device.
Base: *N*=6,400 parents of 6- to 14-year-olds who use the internet, 800 in each country.
Source: Lupiáñez-Villanueva et al. (2016)

2.2 Demographic factors – age, gender, socioeconomic status

The child's age is the main factor that differentiates media access and use, as shown in Table 1 from Ofcom (2016a) below. It appears that:

- nearly all children have internet access at home, but younger children are less likely to use it
- four in ten (41%) children aged 3-4 use the internet at home or elsewhere, rising to 67% of 5- to 7-year-olds, 90% of 8- to 11-year-olds and 98% of 12- to 15-year-olds
- use of the standard TV set shows signs of declining, as does use of the desktop computer, while access to and use of the smart TV set, mobile phone and tablet computer is rising
- most connected devices are more accessible to and used by older than younger children.

Table 1: Summary of children's access to and use of device at home, by age

All children	Aged 3-4		Aged 5-15		Aged 5-7		Aged 8-11		Aged 12-15	
	Access	Use	Access	Use	Access	Use	Access	Use	Access	Use
Standard TV set	85%↓	76%↓	89%	85%↓	85%	80%	92%	88%	90%↓	87%
Tablet computer	81%↑	55%	83%	75%	79%	67%	86%↑	80%	83%	74%
Desktop computer/ laptop/ netbook- with internet access	74%	24%	82%↓	67%↓	80%	49%	79%↓	66%↓	86%	82%
Games console/ player	50%↓	25%↓	75%↓	66%↓	66%↓	52%↓	81%	74%	77%	67%
Digital Video Recorder (DVR)	66%	49%	68%↓	61%↓	63%↓	56%↓	68%↓	59%↓	71%	68%
DVD / Blu–ray player**	64%↓	44%↓	66%↓	56%↓	62%↓	49%↓	67%↓	58%↓	67%↓	59%↓
Radio	55%↓	17%	63%↓	33%↓	56%↓	22%	64%↓	33%	67%	41%
Smart TV set	50%↑	43%↑	52%↑	47%↑	54%↑	46%↑	50%↑	45%↑	52%↑	49%↑
Mobile phone	1%	23%	48%↑	62%↑	5%	28%	43%↑	57%	86%↑	91%↑
E-book reader	21%↓	5%	28%	12%	27%	10%↑	28%	14%	29%	13%
Portable media player	22%↓	5%↓	27%↓	16%↓	24%	9%	25%↓	15%↓	31%↓	22%↓
Any standard/ smart TV	98%↓	92%↓	99%	97%	99%	96%	99%	98%	99%	98%
ANY INTERNET	81%	41%	94%↑	87%	86%	67%	95%↑	90%	98%	98%

QP3: I'm going to read out a list of different types of equipment that you may or may not have in your home, and which your child may or may not use (prompted responses, single-coded). ** Prior to 2016 this question asked about a DVD player/DVD recorder/Blu-ray recorder (fixed or portable).
Base: Parents of children aged 3-4 (684 in 2016) or 5-15 (1,375 aged 5-15, 398 aged 5-7, 503 aged 8-11, 474 aged 12-15 in 2016). Significance testing shows any change between 2015 and 2016.
Source: Ofcom (2016a)[12]

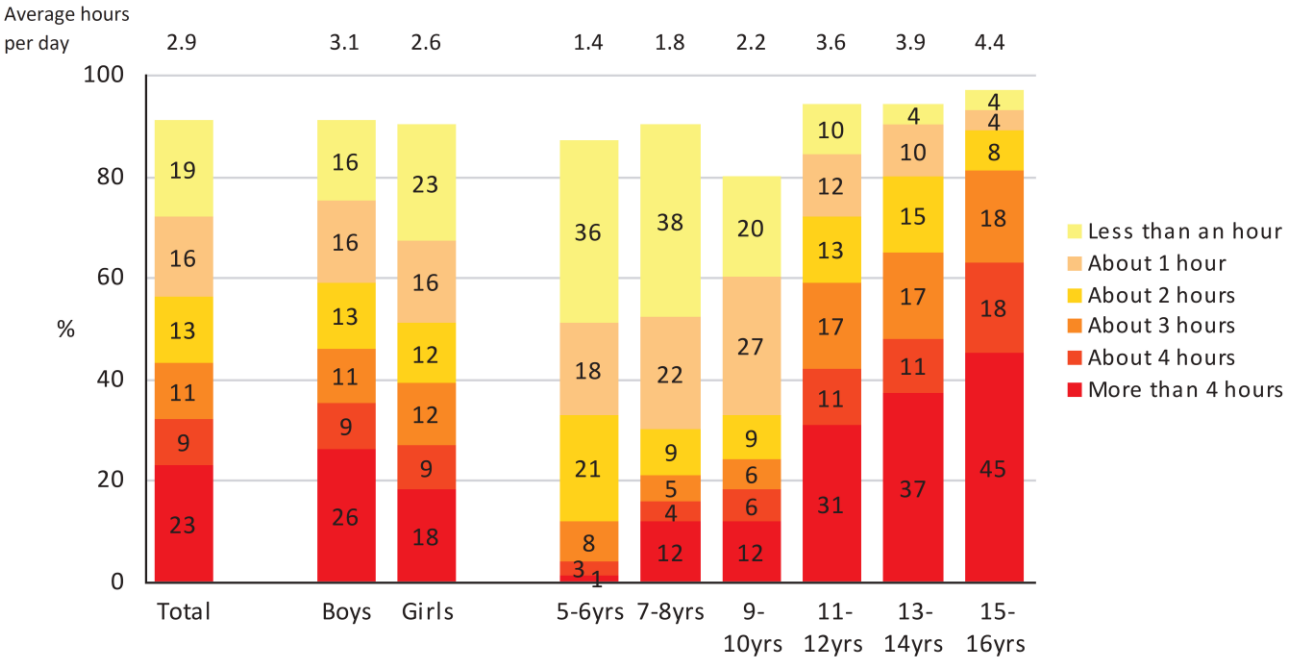
In terms of gender, Ofcom's (2016a) national survey found that more boys than girls own and use games consoles or players, and say they would miss these the most, while for girls the device they would miss most is their mobile. But generally, gender makes less difference in terms of access and use overall. Childwise (2017) findings add to this picture (see Figure 5 below):

- boys spend longer online per day in comparison to girls (3.1 vs. 2.6 hours)
- some children, especially by the age of 15-16, use the internet on average for over four hours per day, while younger children use it much less

[12] Table 1 shows access at home, and use anywhere. For mobile phones the percentages shown in the 'access' columns relate to personal ownership of a mobile phone rather than household ownership. The percentages shown for use are higher than those shown for personal ownership, as this includes use of mobiles within the household that are not directly owned by the child (Ofcom, 2016a, p. 28).

- two in three 7- to 16-year-olds say that going online is important to them, and half of those (one third overall) say it is very important – more boys and more teenagers are likely to consider it quite or very important.

Figure 5: Average time spent online per day, by age and gender



Base: All aged 5-16 (9.0m / unwtd 952)

Source: Childwise (2017)

In a study by Livingstone and Helsper (2007), non-users and occasional users of the internet were more likely to come from working-class families, while frequent users were more likely to come from middle-class families with better quality internet access and, as a consequence, more advanced digital skills. Pursuing digital inequalities among children – or households with children – remains an evidence gap, and few surveys examine children's media use in relation to SES.

Ofcom (2016a, p.23) contrasted the poorest (DE) and wealthiest (AB) households:

> Children aged 5-15 in DE households are less likely to have access to and to use a wide range of devices; the reverse is true for those in AB households. However, they are no less likely to have access to or use a mobile phone, or to have their own tablet or mobile phone, and are more likely than the average to use a standard TV set.

As Table 2 from Net Children Go Mobile (Livingstone et al., 2014a) further shows:

- internet use is becoming more private – in the child's own room, or when out and about, as children grow older
- SES matters considerably, with children from low SES homes making less daily use of the internet in all locations, at home, school and elsewhere
- children from low SES homes are less likely to say that there are lots of good things for them to do online. They also report having significantly fewer digital skills than their better-off peers.

Table 2: Daily internet use in different places, by gender, age and SES

	% own bedroom	% at home but not own room	Use at home (bedroom or elsewhere)	% at school	% other places	% when out and about
Boys	63	66	81	25	18	33
Girls	65	60	76	34	27	32
9-10	20	33	37	18	3	3
11-12	47	73	78	40	16	8
13-14	76	60	90	20	24	34
15-16	96	80	97	38	38	71
Low SES	47	53	65	16	7	17
Medium SES	76	59	82	30	28	43
High SES	66	73	85	37	27	35
All	64	63	79	29	22	32

NCGM: Q1 a-e: Looking at this card, please tell me how often you go online or use the internet (from a computer, a mobile phone, a smartphone, or any other device you may use to go online) at the following locations....
Base: All children who use the internet. UK survey for Net Children Go Mobile.
Source: Livingstone et al. (2014a)

2.3 Summary

The recent time trends in children's internet use are as follows:

- There is increasing internet use among very young children.
- An increasing amount of time is spent per week by internet users.
- There has been a shift from shared to personal devices for internet use (although younger children prefer use of the tablet).
- UK children are more likely to use the tablet than children in other European countries; they are also more likely to use the internet at school.
- Age is the major factor that differentiates among children in terms of amount and context of internet use.
- Gender matters more to patterns and preferences in internet use rather than to access.
- Despite increasing access and use among children, socio-demographic inequalities persist.

3. Children's online activities

3.1 Main findings and trends over time

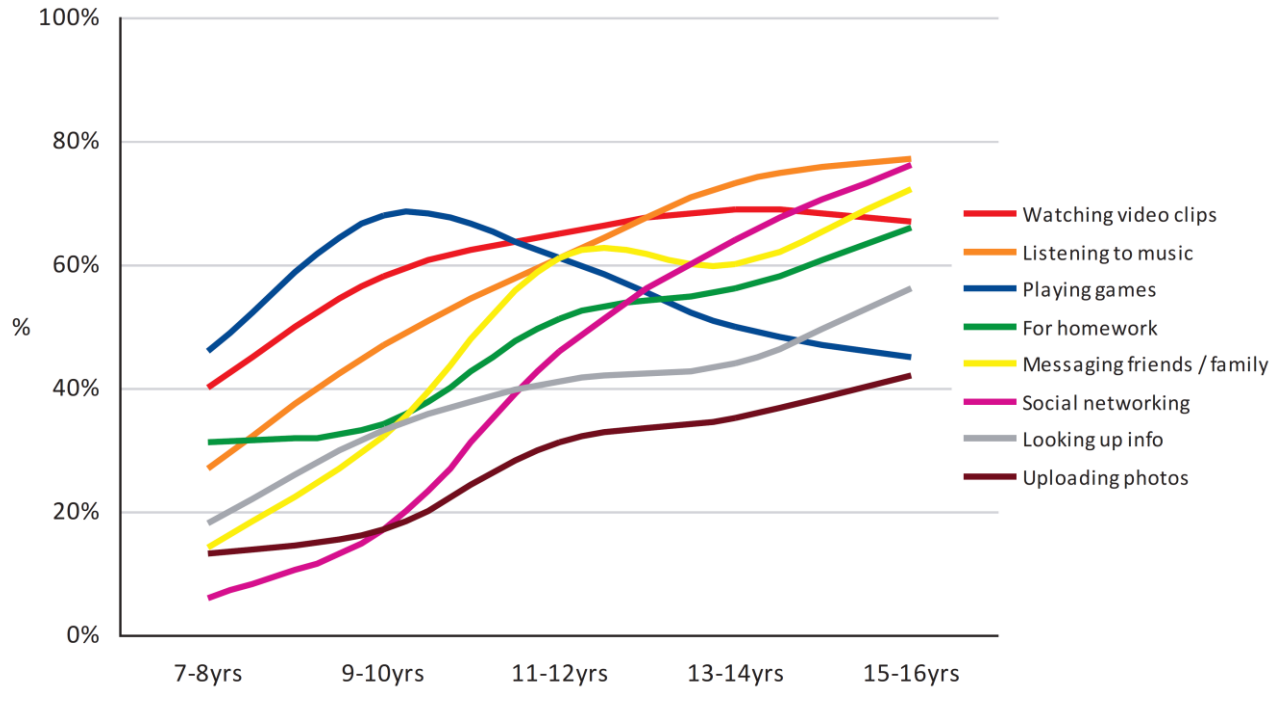
Digital technology and the use of the internet is becoming an integral part of children and young people's lives. Broadly speaking, the more and better quality children's access, the deeper and more diverse are their online activities (Livingstone et al., 2012a). Although our present focus is more on risks than opportunities, it is important to understand children's positive motivations for and choices in using the internet. This will, in turn, help us to understand how they use the internet and how this may have consequences for their wellbeing.

It is also important to realise that online activities cannot be easily divided into 'opportunities' or 'risks'. Children undertake a range of what might be called 'risky opportunities' – often associated with social networking (Livingstone, 2008). Arguably, positive experiences as well as risky opportunities and even risk can contribute to children's digital literacy and resilience (see later).

Research shows that children use the internet for a variety of reasons. This is especially true for older children who use it more broadly (e.g., social networking, uploading photos, homework) in comparison to younger children who use it for more specific reasons (e.g., watching videos).

For example, Childwise's (2017) Monitor Report found that children aged 7-16 use the internet to watch video clips (59%), listen to music (56%), play games (54%), complete homework (47%), interact with family and friends (47%), social networking (40%), look up information (38%), and upload videos, photos and music (27%). As children get older, music and communication become more important while playing games declines (see Figure 6 below).

Figure 6: Reason for going online, by age



Base: All aged 7-16 (7.4m / unwtd 1736)

Source: Childwise (2017)

3.2 Online opportunities

As children's frequent engagement in video, music, gaming, messaging and searching implies, their internet use is broadly positive. Moreover, research shows that children's online and offline lives are highly intertwined. Ofcom (2016b) reported that children's online and offline activities are integrated as some children use digital technology to complement their offline activities.[13]

The UK Safer Internet Centre (2016a) surveyed 1,500 13- to 18-year-olds in January 2016 about their experiences of online empowerment. Results showed that:

- young people recognise the positive role of the internet in relation to self-expression, developing understanding, bringing people together and respecting and celebrating differences
- the majority of participants (78%) report that they can be themselves online. However, girls are less likely to be themselves online in comparison to boys (74% vs. 82% respectively), and children with disabilities in comparison to children without disabilities (69% vs. 79% respectively)
- 47% of young people use technology to support and promote respect and kindness (e.g., liking or sharing someone else's post, posting supportive comments and signing an online petition). This was more common among girls in comparison to boys (58% vs. 35% respectively).

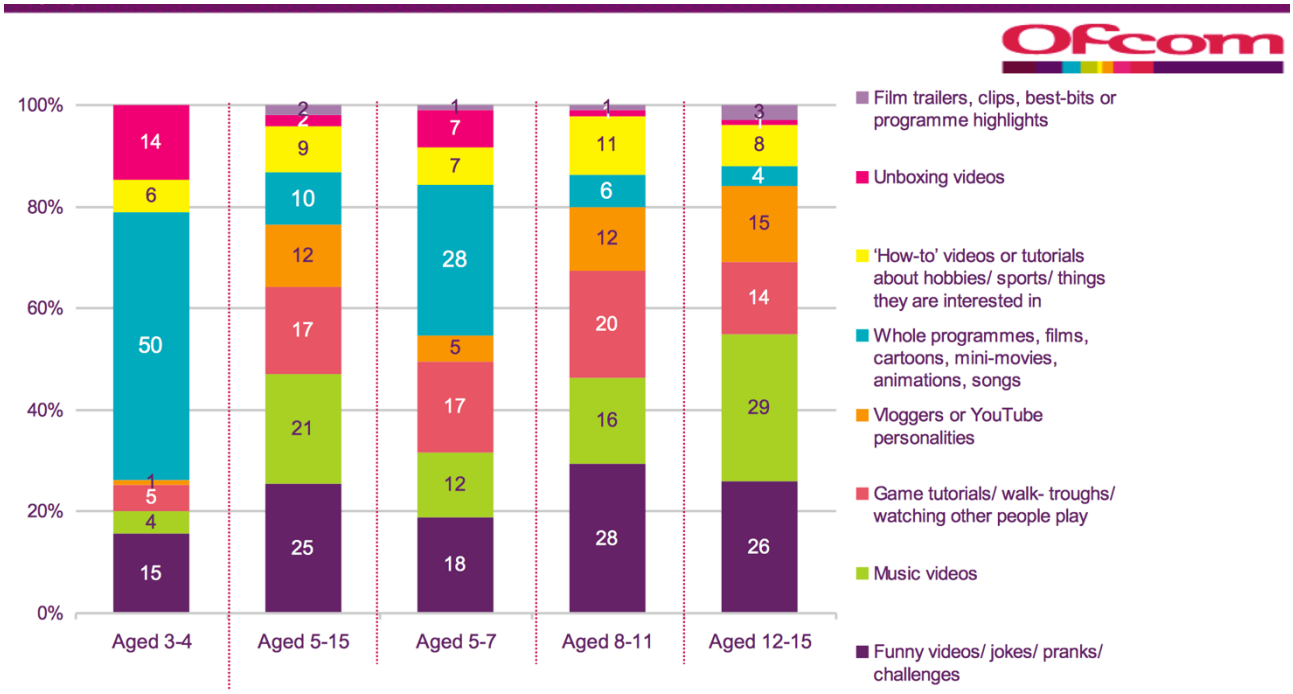
These points are supported by the following quotes from UK Safer Internet Centre (2016a, p. 11):

> "I made an Instagram account to spread female rights, LGBT++ rights, religious rights and more." (Girl, aged 14)
> "I posted a comment in support of someone who was being picked on for being Black." (Boy, aged 15)
> "I try my best to only follow/friend etc people who only treat others with respect and kindness; if I saw that someone was abusive or bullying or posting hate, I would always unfollow them." (Girl, aged 17)

Parents of 3- to 4-year-olds report that their child is more likely to watch TV programmes, films, cartoons, mini-movies, animations or songs on YouTube. The content children watch as they grow older differs as older children watch more music videos, vloggers or YouTube personalities and funny videos (Ofcom, 2016a) (see Figure 7).

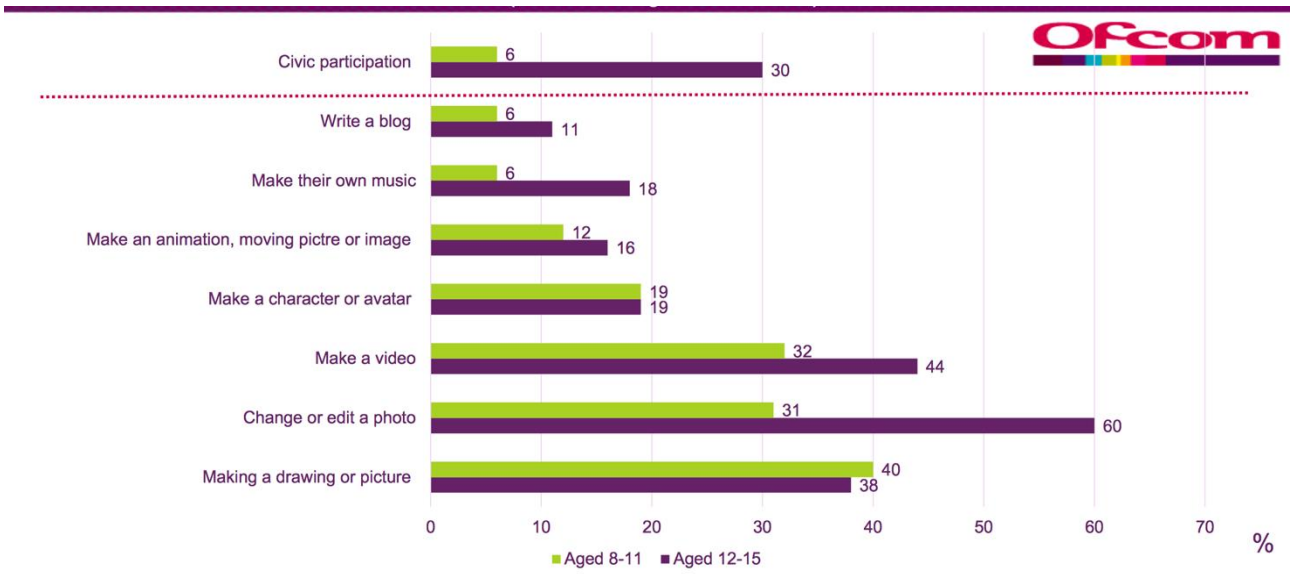
[13] Ofcom's results from in-depth research with 17 children showed that children who have active offline social lives use the internet to enhance their experience, knowledge and skills. Parents who encouraged their children's offline lives were more likely to engage in purposeful internet usage (Ofcom, 2016b).

Figure 7: Favourite types of content watched on YouTube website or app, by age



QP22D/QC7B: And which one of these things is their favourite thing to watch on YouTube? (prompted responses, single-coded) Responses from parents of 3-7s year olds and from children aged 8-15.
Base: Parents whose child uses YouTube website or app aged 3-4 (246 in 2016) or 5-15 (207 aged 5-7, 358 aged 8-11, 409 aged 12-15 in 2016).
Source: Ofcom (2016a)

Figure 8: Online creative activities and creative participation, by age



QC14: When you go online do you ever do things like sign petitions, share news stories on sites like Facebook or Twitter or write comments or talk online about the news? (unprompted responses, single-coded)
QC13: When you use things like computers, tablets, or mobile phones, have you ever done any of these things? This could include any time spent learning about this when you were at school.
Base: Children aged 8-15 who go online (445 aged 8-11, 463 aged 12-15).
Source: Ofcom (2016a, adapted from Figures 46 and 47)

Notably, the internet allows children to be content creators as well as receivers, building their confidence, competence and enabling them to participate in their peer culture and the wider society. Teenagers are much more likely to take up these opportunities than younger children. Figure 8 shows that:

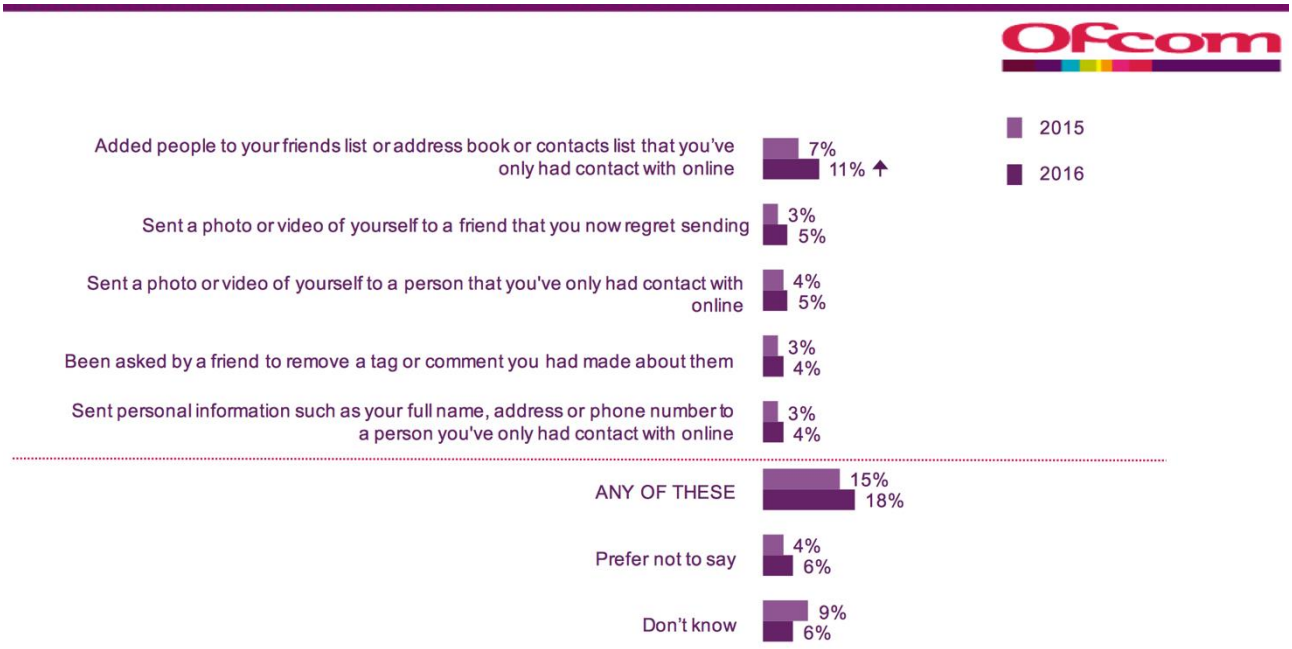
- four in ten 8- to 15-year-olds use digital devices to make a drawing or picture, and around one third of 8- to 11-year-olds rising to nearly two thirds of 12- to 15-year-olds have edited a photo using digital devices. In notably smaller numbers, children also use digital devices to make videos, create their own avatars, create an animation or music or blog
- while such creative expression is less practised by children than the receipt of online content, these remain significant opportunities for children in the digital age
- a third of 12- to 15-year-olds but few 8- to 11-year-olds have undertaken forms of civic participation such as signing petitions, sharing news stories or talking about news online.

3.3 Risky opportunities

Such creative activities can be conducted on a range of sites and services, including social networking sites (SNSs) and video-sharing sites, as well as in multiplayer games or other digital services. While children and adults regard many of these activities in positive terms, taking up online opportunities can, in and of themselves, be risky. Adding new people to one's contacts, for instance, may be a great way to make new friends, but can also bring children into contact with potentially abusive strangers.

With these risky opportunities in mind, Ofcom's surveys have tracked the incidence of a range of risky online behaviours, as shown in Figure 9. This shows that only a small minority of children say they have added contacts they don't know offline, or sent photos they now regret, or disclosed personal information online. Indeed, fewer than one in five 12- to 15-year-olds say they have done any of the risky online behaviours asked about.

Figure 9: Potentially risky online behaviour among children aged 12-15, 2015 and 2016



QC60: Please take a look at the list of things shown on this card and think about whether you have done any of these things in the last year. If there is something on the list that you have done in the last year then please just read out the numbers from the card (prompted responses, multi-coded).
Base: Children aged 12-15 who go online at home or elsewhere (463 in 2016).
Source: Ofcom (2016a)

Over the past decade, social networking activities have quickly become of major importance to children, with the specific sites available – in terms of how they enable peer-to-peer interaction, and which sites are fashionable or popular and why – continuing to change and innovate over the years. In the 2012 UKCCIS review, the focus was on how children used Facebook, Bebo and MySpace. Platforms and services have changed in brand and number, and many children are now using multiple social networking services. However, under-age use, variation in use of privacy settings, contact with large numbers of 'friends' – these and related practices remain risky.

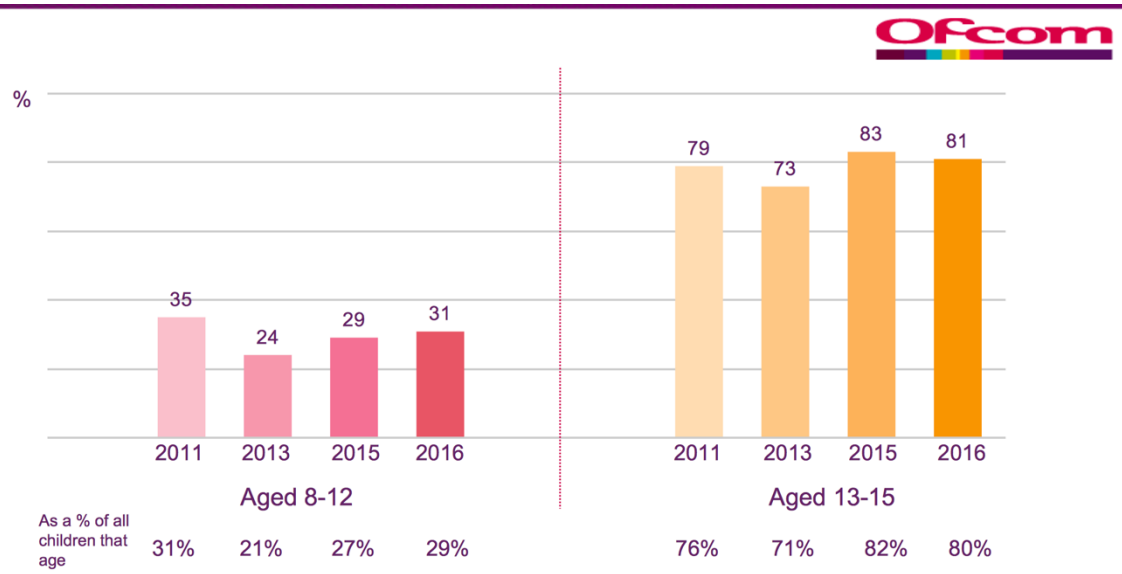
According to a survey conducted by Clarke and Crowther (2015) with 11 primary schools and 19 secondary schools, half of secondary pupils and over a quarter of primary pupils have communicated with people they do not know when using social media.

Particular policy attention has focused on the degree to which children use SNSs when they are 'under age' in terms of most sites' terms and conditions (usually 13 years old, following the US Children's Online Privacy Protection Act 1998).

- Figure 10 suggests that such regulation is broadly effective insofar as far more teenagers than younger children have an active social media profile (Ofcom, 2016a), although it may also be that younger children are simply not interested in social networking.
- However, it is not insignificant that over a quarter of 8- to 12-year-olds use SNSs, and there is little evidence of a reduction in this proportion, despite efforts by industry and policy-makers.
- NSPCC findings (Lilley & Ball, 2013) suggest that 59% of UK 11- to 12-year-olds have social media accounts, and 23% of those have encountered something nasty online.

- Also interesting is that one fifth of young teenagers do not use SNSs, despite the popular perception that they all do so. Again, there is little change in recent years.

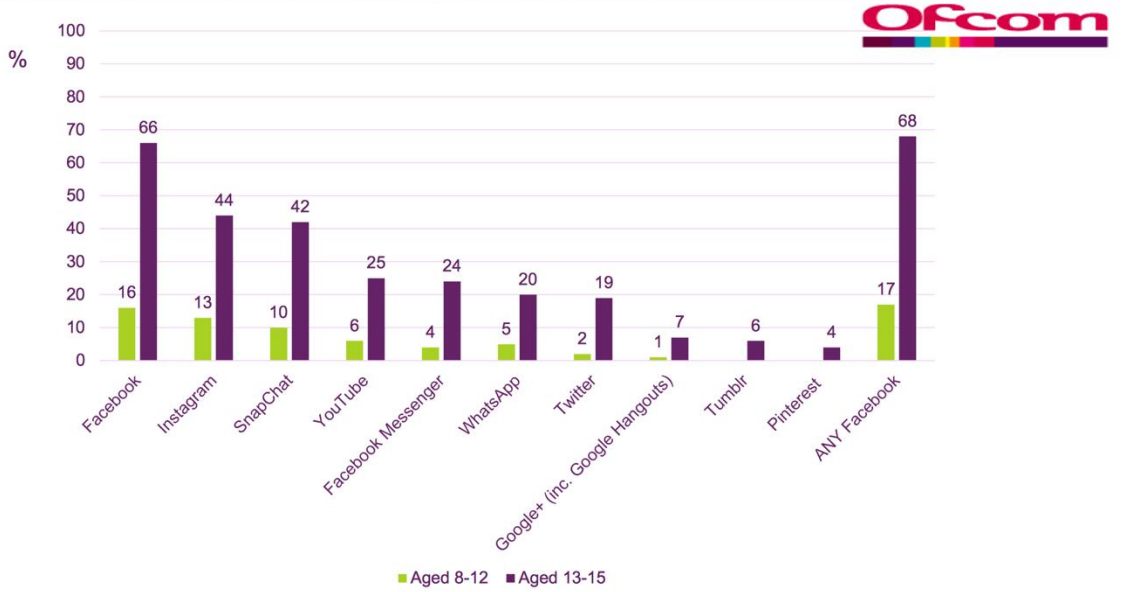
Figure 10: Children who go online with an active social media profile, by age, 2011, 2013, 2015 and 2016



QP43/QC19: I'd now like to ask you some questions about your child's use of social media – websites or apps like Facebook, Twitter, Instagram, Tumblr, Snapchat, WhatsApp and some activities on YouTube. Does your child have a social media profile or account on any sites or apps? (prompted responses, single-coded)
Base: Children aged 8-15 who go online (584 aged 8-12, 324 aged 13-15 in 2016). Significance testing shows any change between 2015 and 2016.
Source: Ofcom (2016a, adapted from Figures 36 and 37)

Figure 11 examines which social media sites are favoured by younger and older children. Contrary to the popular view that Facebook is no longer fashionable, it is clear that this is, nonetheless, the most popular social media site for UK children. This is followed by Instagram and Snapchat, also used in small but significant numbers by 'under-age' children as well as teenagers.

Figure 11: Social media sites or apps used by children, by age



Q20: Which social media site do you use? (unprompted responses, multi-coded) Responses from parents from 5-7 year olds and from children aged 8-15.
Base: Children aged 8-15 (646 aged 8-12, 331 aged 13-15).
Source: Ofcom (2016a, adapted from Figures 38 and 39)

Research conducted by the NSPCC (2016d) with a non-random sample of 1,700 children and 700 parents and carers of 8- to 14-year-olds explored attitudes towards social networks, apps and games. The research found that the children rated the following sites as the riskiest:

- Chatroulette – 100%
- Sickipedia – 100%
- Omegle – 89%
- ASK.fm – 86%
- Tinder - 76%
- MeowChat – 67%

Children stated that they were most likely to see sexual, violent and other harmful content on the following sites:

- Self-harm: ASK.fm
- Violence: Call of Duty
- Bullying: ASK.fm
- Sexual: DeviantArt, Omegle

3.4 Summary

Research on children's online activities reveals that:

- Children go online for many reasons, and these change over time, shifting broadly from engaging with mass-produced content to also engaging with online communication.
- Children are generally very positive about their online experiences, and relish the chance to be constructive digital citizens.

- Although the internet affords many opportunities to be content creators as well as receivers, only a minority of children take up these opportunities to create or to engage civically online.
- Although the internet also affords opportunities for risky online behaviour, the levels at which children report such behaviour are generally low.
- However, the use of SNSs by under-age children, and the range of services they use means that some are communicating online without protection or supervision appropriate to their age and need.

4. Risk of harm to children online

4.1 Understanding risk and harm

It is increasingly accepted that, as with children riding a bicycle or learning to swim, using the internet will carry some risk of harm. The policy task, then, is not to eliminate all risk, but to manage risk so that children are prepared for and can learn from milder risks, while resources are also used to minimise harm, especially from severe risks. The research task is to identify which circumstances pose what kind of risk, which factors mean that risk is increased or reduced, and when risks do or do not result in tangible harm (Livingstone, 2013).

Risks do not inevitably result in harm, but rather concern factors that raise the probability of harm to children (Livingstone, 2013). In this section we review evidence regarding the range and incidence of different types of risk encountered by children on the internet.

The 2012 UKCCIS review called for more research on the following areas:

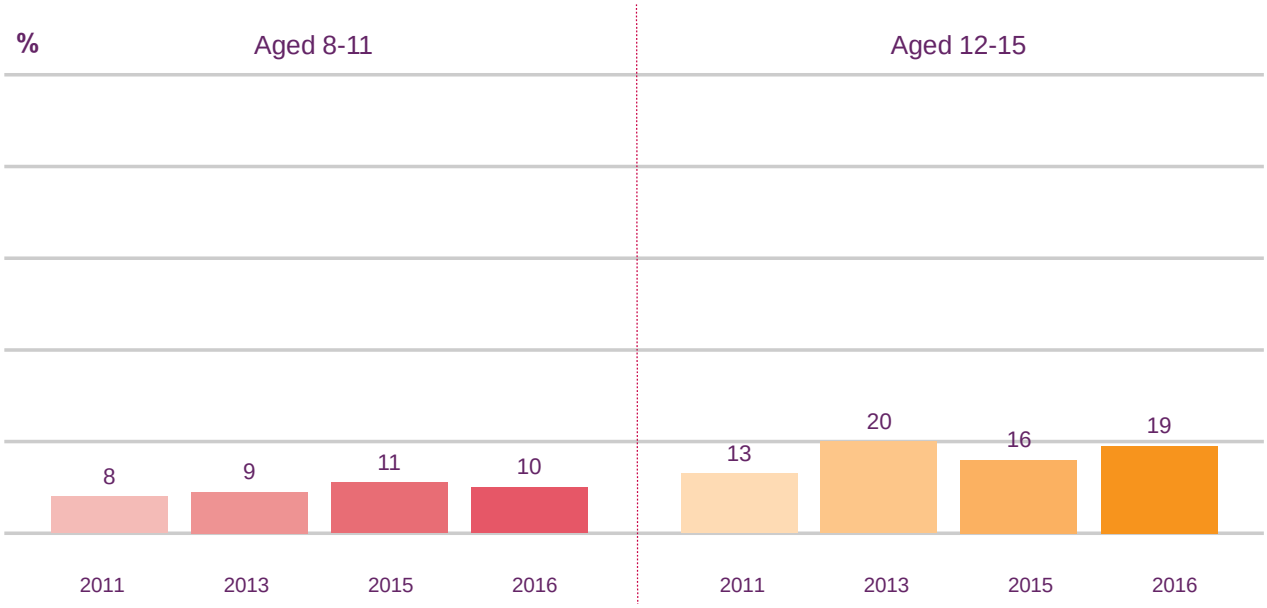
- Online risks faced by younger age groups from 5-11 in order to inform the development of future educational strategies for schools, parents and young people.
- Implications of increased internet access using portable devices (such as laptops, mobile phones, gaming consoles and portable media players) to access online content, and whether this may increase online risks.
- The extent to which different types of vulnerable young people, such as those with special educational needs (SEN), disabilities, or socioeconomic disadvantages, are more or less likely to face online risks, how they respond to risks and how they can be best supported.

In the past five years, research on some but by no means all of these topics has been conducted. We begin, however, with children's own accounts of how often children report experiencing something upsetting online.

4.2 How many children report online risk?

In the past year, around one in ten children who use the internet aged 8-11 and almost twice as many (19%) aged 12-15 say that they encountered something online that they found worrying or nasty in some way that they didn't like (Ofcom, 2016a). This proportion has changed little in the past five years (see Figure 12).

Figure 12: Child's claimed experience of having seen any online content in the past year that was considered worrying or nasty, by age, 2011, 2013, 2015 and 2016



QC29: And in the last year, have you seen anything online that you found worrying or nasty in some way that you didn't like? ** Previously asked about 'worrying, nasty or offensive'. (prompted responses, single-coded)
Base: Children aged 8-15 who go online (445 aged 8-11, 463 aged 12-15). Significance testing shows any change between 2015 and 2016.
Source: Ofcom (2016a)

4.3 What do children find upsetting online?

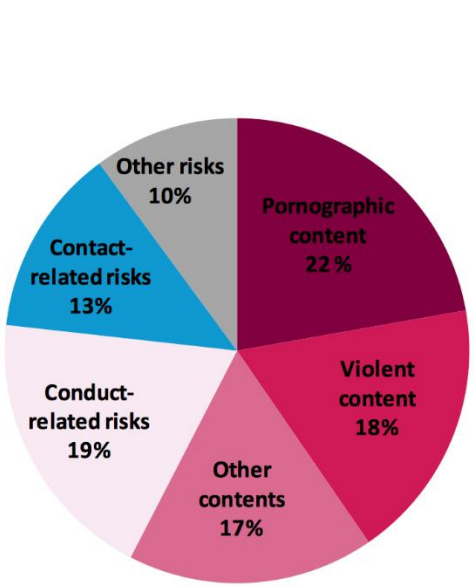
EU Kids Online asked children across Europe in 2010-11 to describe what upset them online – selected answers are shown in Figure 13 below (see Livingstone et al., 2014b).

Figure 13: What European children find upsetting online

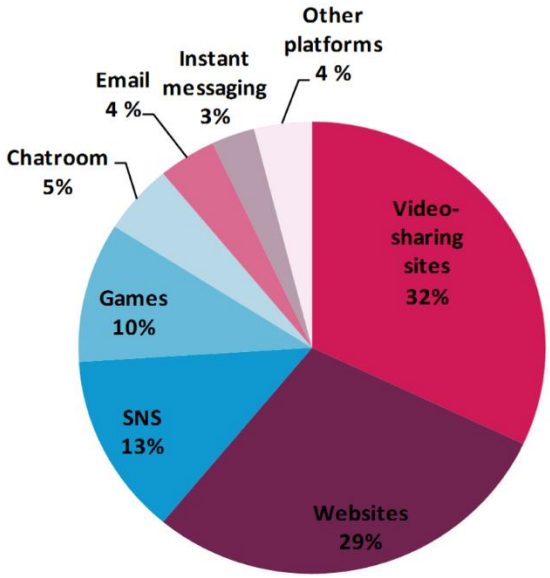
Source: EU Kids Online (Livingstone et al. 2014b)

Pornography and violence constituted a substantial part of children's concerns. As children explained, they mostly encountered such upsetting content on video-sharing sites such as YouTube and on SNSs (Livingstone et al., 2014b) (see Figure 14).

Figure 14: Which risks bother European children online, and where they encountered them



Base: 9-16 year olds in Europe who identified one or more risks online (N=9,636)



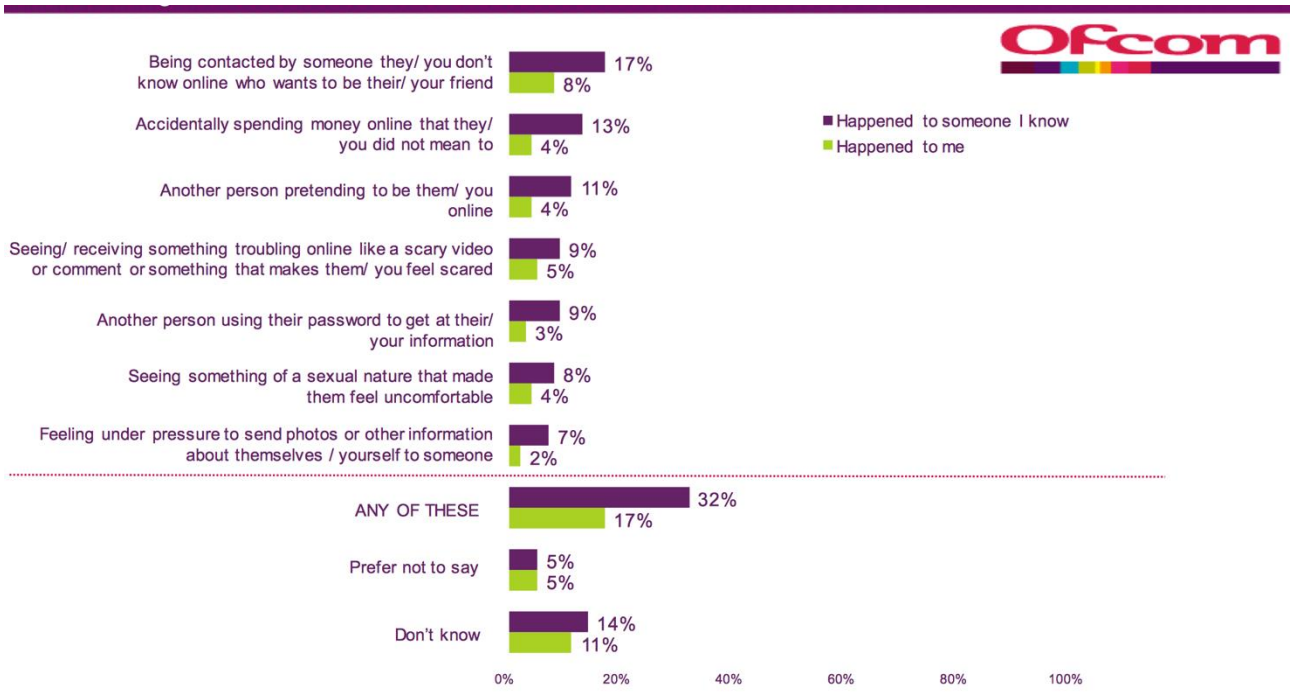
Base: 9-16 year olds in Europe who mentioned a platform when describing online risks (N=4,356)

Source: EU Kids Online (Livingstone et al, 2014b)

Ofcom has since pursued what worries children in relation to mobile phones (see Figure 15):

- being contacted by someone they don't know, who wants to be their friend, is the most commonly reported negative experience, although only 8% of 12- to 15-year-olds say this has happened to them
- only 4% say they saw something sexual online that had made them feel uncomfortable and only 2% felt under pressure to send a photo
- notably, twice as many report the negative experiences as having happened to someone they know compared with it happening to them. This may explain why the popular perception of online risk is of higher incidence than Ofcom's figure suggests.

Figure 15: Experience of negative types of online/mobile phone activity among children aged 12-15

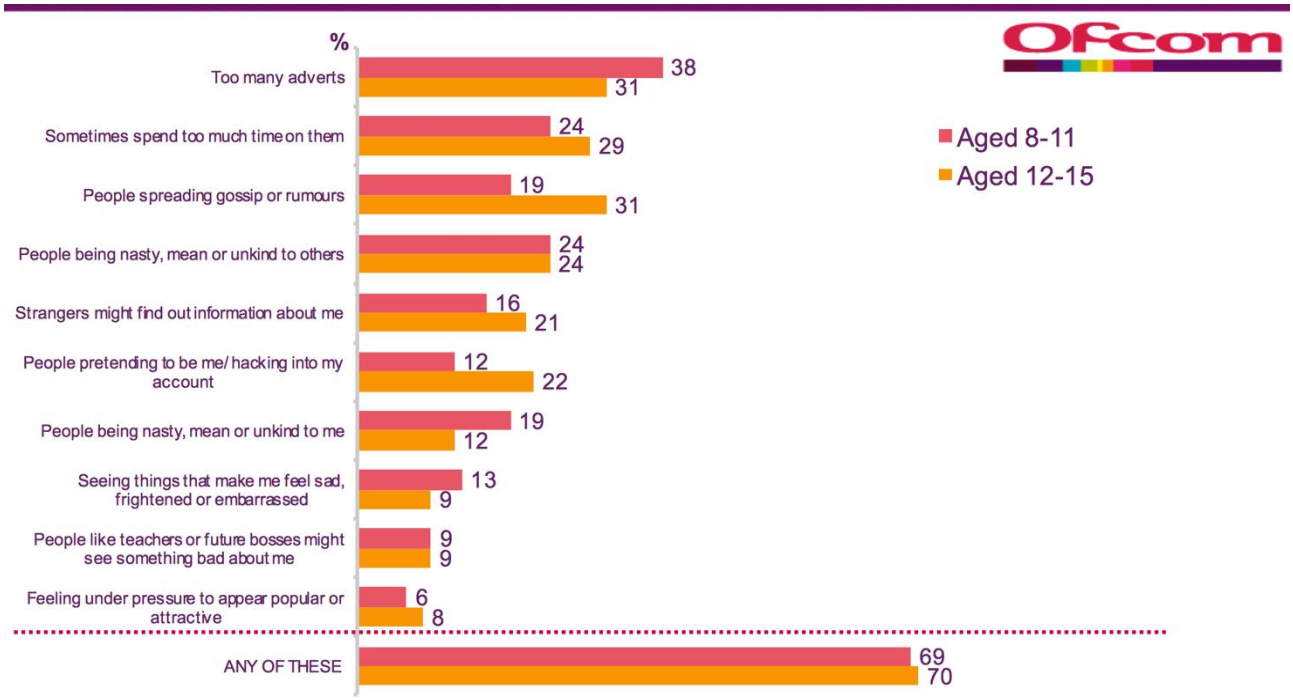


QC58/QC59: Please take a look at the list of things shown on this card and think about whether they have happened to anyone you know in the last year, either online or on a mobile phone. Again, please just read out the numbers from the card if any of these things have happened to you in the last year (prompted responses, multi-coded).
Base: All children aged 12-15 (474 aged 12-15 in 2016).
Source: Ofcom (2016a)

Ofcom also asked children what they disliked about social media sites and apps (see Figure 16):

- There being 'too many' online advertisements is children's top concern, especially among 8- to 11-year-olds.
- This is followed by a concern that they themselves spend too much time on social media.
- Gossip and rumours particularly concerned 12- to 15-year-olds, while a quarter of both age groups (8-11 and 12-15) disliked how people are nasty or unkind on social media.
- Few, by contrast, appear concerned that their digital footprint could be problematic for them later, and few said they felt under pressure to appear popular or attractive online.

Figure 16: Dislikes about social media sites or apps, by age

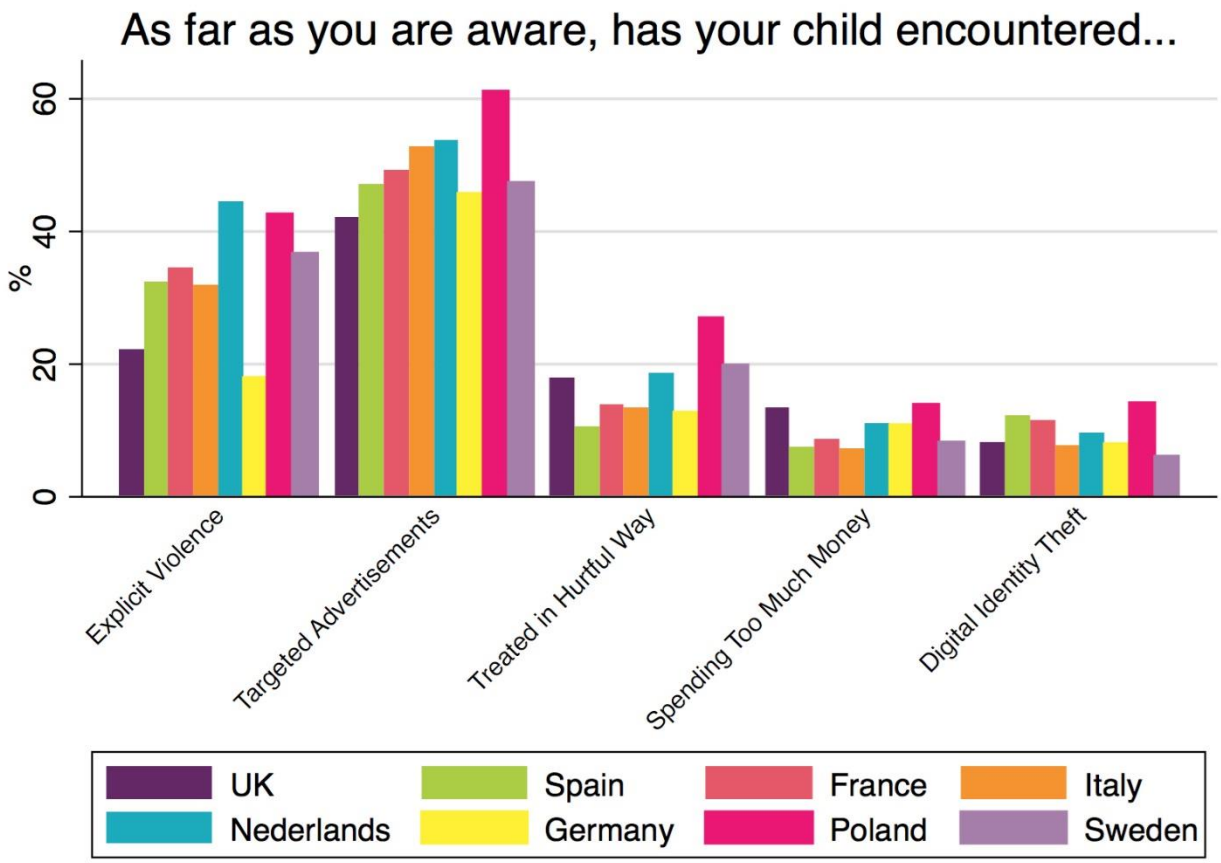


QC22: Which of these things, if any, don't you like about social media sites or apps? (prompted responses, multi-coded)
Base: Children aged 12-15 who go online at home or elsewhere and have a social media site account (104 aged 8-11, 335 aged 12-15 in 2016).
Source: Ofcom (2016a)

Where does the UK stand in relation to other European countries in terms of online risks experienced by children? From a recent European survey of parents (Lupiáñez-Villanueva et al., (2016), as shown in Figure 17 below, it seems that:

- experiencing targeted (or personalised) advertising is fairly common, as is encountering explicit violence online
- being treated in a hurtful way, spending too much money, digital identity theft and the other risks asked about are all much less common
- the UK does not stand out as distinctively high or low, in terms of children's online experiences or risks as reported by their parents.

Figure 17: Parents' perception of the types of risks encountered by their children online, by country



Q19: For the following situations, please indicate, as far as you are aware, whether or not your child has encountered them in the PAST YEAR? (a) Seeing images on the internet that contain explicit violence against others, (b) Being exposed to personalised/targeted advertisements (e.g., in social media, Google searches etc.), (c) Being treated in a hurtful or nasty way on the internet by another child or teenager (this includes being teased repeatedly in a way he/she did not like, or being deliberately excluded or left out of things), (d) Spending too much money on online games or in-app purchases, (j) Digital identity theft or identity fraud in which someone wrongfully obtains and uses your child's personal data.
Base: *N*=6,400 parents of 6- to 14-year olds who use the internet, 800 in each country.
Source: Lupiáñez-Villanueva et al. (2016)

4.4 Classifying and measuring risk of harm

In this section we examine evidence on children's experiences of a range of risks of harm. We do so by broadly following the categories outlined by EU Kids Online, as shown in Table 3 below. This classifies the kinds of risk that children may encounter online, also recognising that risks vary depending on how the child interacts with the digital environment.

- Broadly, online risk occasions concern in relation to aggression and violence of various kinds, sexual harms to children, problems associated with inappropriate or damaging values and commercial/persuasive risks. Table 3 shows illustrative examples only, and inevitably these will continue to change and evolve. For example, by potentially harmful user-generated content one can think of self-harm websites or information about methods of suicide or encouragement to anorexia or bulimia. Other problems occur, although most are yet to be researched.
- The second dimension of the table focuses attention on the role of the child. This acknowledges children's agency in relation to online interactions – as a *recipient* of mass-

produced content, as a *participant* in a peer- or adult-initiated interaction, or as an *actor* who contributes in producing risky content or contact. The intent is not to blame children for bringing risk onto themselves in any simple sense but rather, to recognise the complex set of relationships that occur online, with content, with adults, and with other children.

Table 3: A classification of online risks to children

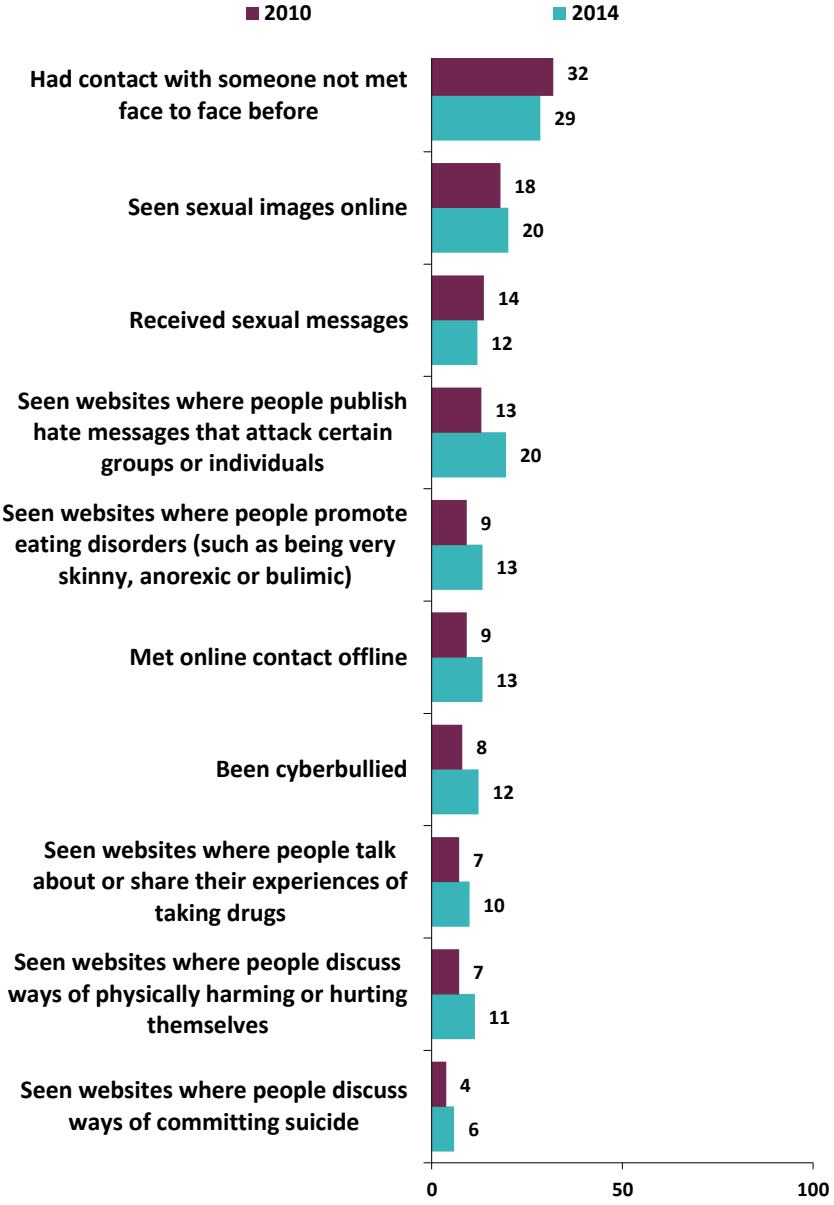
	Content Child as receiver (of mass productions)	**Contact** Child as participant (adult-initiated activity)	**Conduct** Child as actor (perpetrator / victim)
Aggressive	**Violent / gory content**	**Harassment, stalking**	**Bullying, hostile peer activity**
Sexual	**Pornographic content**	**'Grooming', sexual abuse on meeting strangers**	**Sexual harassment, 'sexting'**
Values	**Racist / hateful content**	**Ideological persuasion**	**Potentially harmful user-generated content**
Commercial	**Advertising, embedded marketing**	**Personal data exploitation and misuse**	**Gambling, copyright infringement**

Source: EU Kids Online (Livingstone, Haddon, Görzig, & Ólafsson, 2010)

Among 11- to 16-year-old children who use the internet in Belgium, Denmark, Italy, Ireland, Portugal, Romania and the UK, surveyed by EU Kids Online in 2010 and Net Children Go Mobile in 2014, the incidence of risk is shown in Figure 18 below:

- The 'risky opportunity' of contacting someone not known face-to-face is fairly common.
- The incidence of exposure to pornography and sexting has changed little in recent years, but children appear more exposed to hate messages.
- There is also a slight increase in the reporting of pro-anorexia and other kinds of self-harm sites.

Figure 18: Incidence of risk among 11- to 16-year-old children who use the internet in Belgium, Denmark, Italy, Ireland, Portugal, Romania and the UK, 2010 and 2014



Source: Livingstone et al. (2014c), from EU Kids Online and Net Children Go Mobile data

4.5 Summary

Risk of harm to children can be summarised as follows:

- Risks do not inevitably result in harm, but it is vital to understand the factors that give rise to the probability of harm to children.
- A minority of children (10% of 8- to 11-year-olds and 19% of 12- to 15-year-olds) report having seen something worrying or nasty online in the past year (Ofcom, 2016a).
- Children say they are most likely to encounter upsetting content on video-sharing sites like YouTube, followed by other websites including SNSs.
- Too many advertisements are children's top concerns on social media and apps.
- The UK is neither especially high nor low in relation to other European countries with regard to children's online risks or negative experiences as reported by their parents.

5. Bullying, aggression and hate

Children and young people's ability to use the online environment and associated applications to harass and intimidate each other continues to be of concern to parents and teachers, as well as children and young people themselves. This section reviews the available UK evidence base that has developed since the 2012 UKCCIS review was published.

5.1 Prevalence

Ofcom's 2016 *Children and parents: Media use and attitudes* report included a number of questions about children's experiences of bullying, including online bullying (Ofcom, 2016a):

- 11% of 8- to 11-year-olds and 13% of 12- to 15-year-olds reported being bullied in the past 12 months
- face-to-face bullying is more frequent (6%) for children aged 8-11 than via social media (2%) or group chat/text messages (1%)
- 12- to -15-year-olds report similar levels of bullying across all three contexts (6%)
- 2% of those aged 8-11 and 12-15 also reported being bullied via online games.

Higher prevalence rates were reported in another study examining prevalence of bullying and cyberbullying in a larger sample of 11,166 children aged 14-15 in the UK (Lasher & Baker, 2015). This research found that:

- 11% of the children experienced cyberbullying by phone or online
- girls are more likely to report this form of victimisation than boys (15% compared with 7% respectively).

Research conducted by the UK Safer Internet Centre (2017) examining the role of images in the digital lives of a representative sample of 1,500 children and young people aged 8-17 found that:

- 22% of the sample said someone had posted an image or video to bully them; this didn't vary by age or gender
- 38% reported experiencing negative comments on a photo they had posted online
- this was more frequent in older age groups (32% of 8- to 12-year-olds compared to 45% of 13- to 17-year-olds)
- there were no gender difference in the proportion of children and young people reporting this experience (37% of girls compared with 39% of boys)
- 40% of the sample said that they sometimes don't post images because they are concerned about receiving negative comments.

These results are generally consistent with a recent academic review finding that 15% of children and young people have engaged in the behaviour[14] (Modecki et al., 2014). They are also similar to prevalence figures reported in the 2012 literature review that found that 21% of UK children said they had been bullied, but only 8% reported that this occurred online.[15]

The wider academic literature reports few gender or age differences in the prevalence of cyberbullying, and any identified in specific studies are likely to reflect variations in participant age ranges, sampling and measurement procedures used (Kowalski et al., 2014; Tokunaga, 2010).

[14] Aggregated sample of 80 studies.

[15] For the original research, see Livingstone et al. (2010).

There is a lack of available evidence in the UK examining prevalence of children and young people engaging in cyberbullying behaviours. However, the academic research review by Modecki et al. (2014) found that 16% of them admit having cyberbullied others.

5.2 Risk factors

The academic literature on cyberbullying has examined risk factors for cyberbullying perpetration and victimisation. A wide variety of predictors of these behaviours has been identified. For example, recent reviews have identified anger and risky online behaviour as risk factors for victimisation, and experiencing cyberbullying and normative beliefs about aggression as predictors of perpetration (e.g., Modecki et al., 2014; Zych et al., 2015). This suggests that there is an overlap between victimisation and perpetration that is likely to reflect some involvement of retaliation and escalation in behaviour.

5.3 Experiences and impacts

A variety of psychological and social impacts have been identified as the result of experiencing cyberbullying. These include the experience of emotional distress and anxiety, loneliness and depression, suicidal ideation and self-harm (Kowalski et al., 2014; Zych et al., 2015; see also Daine et al., 2013). This is consistent with the results of an online questionnaire study conducted by Lilley, Ball and Vernon (2014) examining the experiences of 1,024 children and young people aged 11-16 on SNSs. The key findings were:

- 28% of the sample reported an experience that had upset or bothered them when using SNSs in the last year
- of this group, 37% reported experiencing trolling, 22% had been excluded from a social group online, and 18% had experienced aggressive and violent language
- 11% of those who had been cyberbullied reported that this happened every day and 55% at least once a month
- 19% reported being affected by upsetting online experiences for a few days or a week, and 12% for weeks or months
- although the majority of those surveyed tried to deal with the problem themselves, 22% talked to someone face-to-face about their experiences.

The review of Insafe helplines by Dinh et al. (2016) found that the majority of calls they receive from children have a digital or internet component, with cyberbullying and online hate speech being the most frequently reported concerns. Sexual content, abusive communication and racism were also commonly reported.

The negative experiences and impacts of cyberbullying are also highlighted in the *Childline bullying report 2015-16* (NSPCC, 2016a).[16] Key findings were:

- Bullying is one of the most common reasons why children contact Childline, accounting for 9% of all counselling sessions (25,740 sessions in 2015/16).
- A total of 4,541 counselling sessions were delivered about cyberbullying in 2015/16, an increase of 13% from the previous year.

[16] Childline assigns codes to their counselling sessions in order to provide insight into the issues children and young people experience online. This allows them to track the changing trends and issues young people report to them each year. These findings are, however, based on a non-random, self-report sample, and it would be unwise to estimate prevalence trends on the basis of this data.

- Children reported receiving abusive comments about their appearance, sexual bullying and being told to kill themselves. This led young people to feel isolated and unable to understand why others wanted to hurt them.
- Young people also reported feeling pressured into sharing sexual images of themselves, and being threatened with them being posted online, as well as being bullied after sexual images had been shared more widely among their peers. The majority of young people reporting such experiences were girls. This is consistent with the gendered nature of sexting and its involvement in sexual harassment (see later).
- Much of the harassment reported involved peers, often leading to offline harassment at school. This left young people feeling trapped and unable to escape these experiences.
- Some young people talked about experiencing bullying on gaming sites. This was often the result of being less skilled than other players at a specific game, or having accounts hacked and their games ruined. They did not want to tell their parents about what was happening as they were concerned that they would be prevented from playing online as a result.
- The negative impacts of cyberbullying reported to Childline include reduced self-esteem, difficulty in establishing relationships and mental health problems (e.g., self-harm, suicidal thoughts). These impacts are consistent with those identified in the academic literature (e.g., Zych et al., 2015).

Childline quotes the following:

> "I am being bullied by a girl at school. She has taken photos of me and posted them on Snapchat calling me fat and ugly and how I will never have a boyfriend. I have been having suicidal thoughts as this girl is really popular and she has turned my whole year against me." (Girl, 14 years old)
>
> "Every day I wake up scared to go to school, scared about the comments people will make and scared about walking home. Then I get in and log onto my social networking site and there are horrible messages everywhere. It's like there's no escaping the bullies. I'm struggling to cope with how upset I feel so sometimes I cut myself just to have a release but it's not enough. I can't go on like this." (Girl, 13 years old)
>
> "It might sound like not much of a problem but there's this group of people I play with online and they told me to kill myself. I won't kill myself but it upsets me. My parents don't realise how upset it's making me and they tell me to stand up for myself or just not play anymore but they don't know how hard that is! They don't understand why I want to play with people who are not friends, but to me they are. I don't know why they have just suddenly started picking on me but it hurts so much." (Girl, 12 years old)

5.4 Children's concerns and responses to cyberbullying

There is less research addressing how children respond to cyberbullying. Previous studies have identified their use of technological responses (e.g., using block or ignore functions), passive responses (e.g., ignoring, doing nothing) and active help-seeking strategies (e.g., telling friends or parents) (Hinduja & Patchin, 2010; Juvonen & Gross, 2008; Li, 2010).

The way in which young people respond to cyberbullying has also been examined by recent research undertaken by Family Kids & Youth (2017) for the Royal Foundation of the Duke and Duchess of Cambridge and Prince Harry. A series of workshops with children aged 12-15 examined issues related to cyberbullying. Key findings related to concerns and responses were:

- Children described being generally able to cope with the experience of general or random negative comments that are not directly targeted at them. In these situations, many children feel able to deal with their experiences alone and use passive strategies.
- It is when behaviour becomes more personal and targeted that they feel more vulnerable and distressed. In these situations, children are more likely to seek offline help from parents and friends. They may also report their experiences to the relevant social media platform.
- When experiences are persistent and extreme, children can find it difficult to tell anyone, and this exacerbates the negative impacts of their experiences.
- Children had a general awareness of how to make reports on social media, but little knowledge of what action is taken once they are submitted. Many did not receive a response or were disappointed with the outcome.
- This led to a lack of confidence that companies are responding effectively or taking their concerns seriously.

These findings indicate that the nature and perceived severity of cyberbullying influences the coping strategies used by children and young people. Those with direct experience of cyberbullying have an interest in the concept of an online platform that can act as system for available support (Family Kids & Youth, 2016). It also suggests that further attention to reporting processes and outcomes, as well as how these are communicated to children, is required by social media companies.

Quotes from Family Kids & Youth (2017) include:

> "We reported them quite a few times … they didn't do anything about it". (Girl, 8 years old)
>
> "I think they [social media companies] need to like reassure us that we haven't gone unnoticed when we do put in a complaint or whatever 'cos often you feel helpless … you want someone to be there for you." (Girl, 9 years old)

5.5 Online hate

Research examining offline bullying has identified that identity-based harassment (e.g., based on gender and gender identity, sexuality, race, religion, disability status) is also reported by children (Lasher & Baker, 2015).

There is also emerging evidence that children and young people are seeing hate speech online and/or being targeted because of these characteristics in the online environment. Online bullying in relation to gender and sexual harassment is examined in more detail in the next section of the report, but research evidence addressing other forms of hate speech and identity-related cyberbullying is presented below.

There is evidence that a large number of children and young people frequently see hate speech and harassment based on specific identities online. For example:

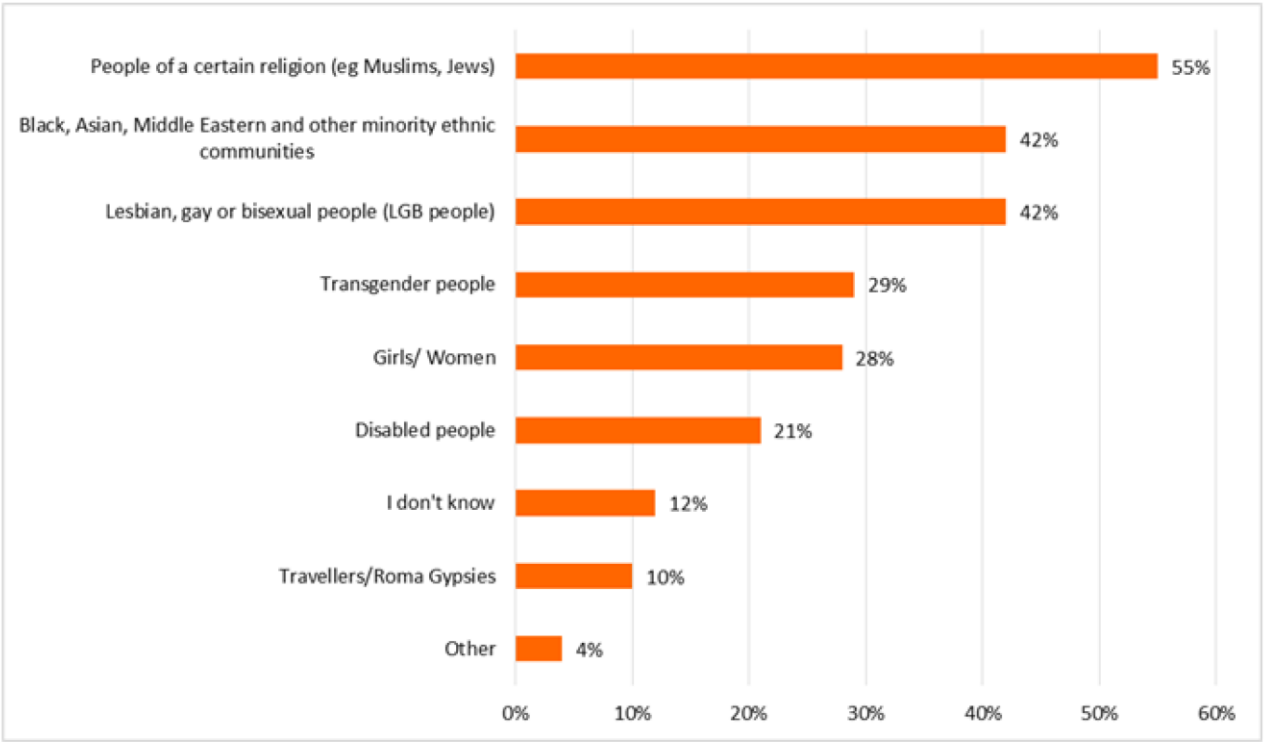
- 64% of children and young people aged 13-17 have seen people posting images or videos that are offensive to a particular targeted group (UK Safer Internet Centre, 2017)
- 34% of children aged 12-15 have seen hate speech directed at a particular group of people online in the previous year (Ofcom, 2016a).

Research conducted by the UK Safer Internet Centre (2016a) using a sample of 1,512 children and young people aged 13-18 found that:

- 82% of the sample had seen or heard online hate speech about a specific group. This was most frequently based on religion, sexual orientation or race (see Figure 19 for frequency across different categories)
- 35% had seen friends posting offensive or threatening things online about people from a specific group
- 24% said they have experienced online hate because of their gender, sexual orientation, race, religion, disability or transgender identity. This did not vary by age or gender
- 46% said that they witnessed something hateful about a certain group on the internet occasionally, while 23% said this happened often and 12% said that it happened all or most of the time
- children and young people with disabilities are more likely to have experienced this (38% compared to 21% of those with no disability)
- those who had this experience reported feeling anger (37%), sadness (34%) and shock (30%) in response
- 74% said that online hate made them careful about what they post online.

This suggests that a large proportion of cyberbullying and online harassment is focused on specific identity-related characteristics. Further research is required to examine the motivations behind such behaviour and educational strategies to challenge related attitudes.

Figure 19: Nature of the online hate that young people were exposed to, by group targeted



Q4a: Which of the following groups have you seen being targeted with online hate? For example, potentially offensive, mean or threatening behaviour on social media, online games or apps. (multiple answers)
Base: All respondents who had reported they had seen something hateful on the internet in the last year (1,241 young people aged 13-18).
Source: UK Safer Internet Centre (2016a)

5.6 Interventions

A key issue relating to educational strategies and interventions that focus on cyberbullying is the need for the evaluation of their efficacy and impact. Despite the wide variety of resources available

that address this behaviour, as well as internet safety more generally, there are few formal evaluations using rigorous methodologies and statistical analyses. Those that have been published have examined programmes developed in other countries and found that the interventions evaluated had successful impacts on attitudes and behaviour related to cyberbullying (e.g., Del Rey, Casas, & Ortega, 2016; Palladino, Nocentini, & Menesis, 2016; Schultze-Krumbholz, et al., 2016).[17]

For example, Palladino, Nocentini and Menesis (2016) conducted an evaluation of the 'NoTrap!' ('Noncadiamointrappola!') programme. This utilised a peer-led approach to preventing and responding to traditional bullying and cyberbullying. The evaluation sample were first year high school students (mean age = 14.91) who took part in two quasi-experimental trials examining the effect of the programme on levels of victimisation and perpetration in both the online and offline environment. Both phases of the study found that the outcome measures remained stable for the control group, but levels of bullying and cyberbullying decreased in the experimental group.

The lack of studies using these methodological approaches in the UK highlights an important direction for future research. Formal evaluation enables a clearer understanding of the efficacy of strategies that focus on preventing and responding to cyberbullying, and their ongoing development to ensure that they realise their intended objectives.

5.7 Current knowledge gaps

The review of the available evidence in this section has identified the following areas requiring further research in order to develop an understanding of cyberbullying among UK children:

- hate speech and identity-based cyberbullying
- perpetrator motivations and characteristics
- bullying through gaming platforms
- the intersection of sexting, sexual harassment and bullying
- efficacy of interventions for preventing and responding to this behaviour.

5.8 Summary

For bullying, aggression and hate:

- Research suggests between 6 to 25% of children and young people in the UK experience cyberbullying.
- The evidence generally indicates a lack of age and gender differences in prevalence.
- There is a lack of evidence about the prevalence of children engaging in cyberbullying behaviours.
- Children and young people can be cyberbullied because of their appearance, gender and sexual behaviour, as well as race, religious belief, disability, sexuality and gender identity.
- The academic literature has identified a number of different risk factors for victimisation (e.g., anger, risky online behaviour) and perpetration (e.g., experiencing cyberbullying, normative beliefs about aggression).

[17] These studies typically utilise research designs in which children and young people are randomly assigned to a group receiving the intervention or a control group that does not. Pre- and post-intervention measures of specific outcome variables (e.g., frequency of victimisation or perpetration) are then taken over a specific period of time. Changes in these factors are compared between the test and control group to determine whether the intervention is effective in reducing victimisation and/or perpetration. There are no published evaluations reporting non-significant evaluations in the literature, but this may reflect the recognised bias in academic research that makes it less likely that studies which do not find significant results are published (Ferguson & Heene, 2012).

- The psychological and social impacts of cyberbullying on children and young people are potentially severe and long-lasting.
- Young people use a variety of different strategies for coping with experiences of cyberbullying.
- They are unsure about the action taken when they make a report about cyberbullying to social media platforms, and some feel that their concerns are not taken seriously.
- There is a lack of published UK research evaluating education and intervention strategies.
- Cyberbullying continues to be a key concern for children and young people, parents/carers and other key stakeholders.

6. Sexting and sexual harassment

6.1 Sexting

The prevalence and impact of children and young people engaging in sexting or creating and sharing sexual images of themselves continues to be a concern for all stakeholders. Despite this, there have only been a small number of studies published examining the prevalence of sexting in children and young people in the UK since the 2012 UKCCIS review.

6.1.1 Prevalence, behaviours and motivations

The most recent research reporting on the prevalence of sexting in England was conducted as part of a study examining the behaviour in the context of the romantic relationships of 724 children and young people aged 14-17 (Wood et al., 2015).[18] The key findings of the study were:

- 38% of the sample had sent sexual images to a partner during or after their relationship, and 49% had received them
- the proportion of the sample sending and receiving sexts increased with age (26% aged 14 compared with 48% aged 16)
- girls were more likely to send sexts than boys (44% compared with 32% respectively), but they were equally likely to receive them
- 51% of the sample indicated that they engaged in sexting to feel sexy/be flirtatious and 45% did so because their partner asked them to
- 20% of the participants who reported sending sexual images indicated that they had been pressured into it. Girls were more likely to report this (27% compared to 7% of boys respectively)
- 98% of the girls who reported feeling pressured experienced negative impacts as a result
- boys were more likely to have positive perceptions of the behaviour compared to girls (91% compared with 41% respectively)
- 32% of the sample reported that their partner subsequently shared images more widely without their consent, with this being much more frequently reported by girls (41% compared with 13% of boys respectively).

[18] This sample was part of a wider European study across five countries. Analysis was only for participants who indicated that they had been in a relationship, which was 75% across the total sample.

Table 4: Sexting behaviours and perceptions

Behaviours and perceptions	Male % (*N*)	Female % (*N*)	Total % (*N*)
Sent image to partner during/after	32 (101)	44 (174)	38 (275)
Received image from partner during/after	47 (148)	49 (192)	48 (340)
Partner shared image	13 (12)	42 (67)	32 (79)
Shared partner's image	15 (22)	13 (24)	14 (46)
Positive perceptions	91 (80)	41 (69)	58 (149)
Negative perceptions	8 (7)	30 (51)	23 (58)
Mixed perceptions	N <5	(50)	2 (51)

Base: Young people aged 14-17 in England in a relationship (*N*=724).
Source: Wood et al. (2015)

The 2012 UKCCIS review reported the results of two studies providing some initial data on the prevalence of sexting:

- A non-representative sample of 535 children and young people aged 14-16 found that approximately 40% reported having friends who engaged in the behaviour (Phippen, 2009). However, as this study did not directly ask young people about their own behaviour, the conclusions that can be drawn are limited.
- The EU Kids Online study reported lower prevalence figures based on a representative UK survey of 11- to 16-year-olds, with 12% having received a sexual message online (Livingstone et al., 2010).

Variations in prevalence between different studies are likely to reflect differences in definitions and measurement, as well as sampling and methodology (Cooper et al., 2016; Klettke, Hallford, & Mellor, 2014). However, the available evidence suggests that some children and young people are engaging in this behaviour and are therefore at risk of the potentially negative emotional and social consequences that can result.

6.1.2 Impacts and consequences

Key concerns about sexting relate to non-consensual forwarding to peers or images being posted online, and the associated social and emotional consequences (Ringrose et al., 2012; van Ouytsel et al., 2015). This includes distress, humiliation and reputational damage, as well as online and offline peer harassment and unwanted sexual advances.[19] This is also examined later in Section 8 on online grooming and indecent images.

These negative experiences and impacts are reported by practitioners and evidenced by data provided by support services and helplines for children and young people:

- Research exploring data from NSPCC helplines (NSPCC, 2016b)[20] indicated that sexting was discussed in 1,392 counselling sessions with children and young people during that year, a 15% increase on the previous year.

[19] Young people's reports about their posting of sexual images online links this practice to the experience of non-consensual sharing and the potential for unwanted sexual solicitation (CEOP, 2013).

[20] Childline assigns codes to their counselling sessions in order to provide an insight into the issues children and young people experience online. This allows them to report the changing trends and issues that children report each year.

- The majority of counselling sessions focused on sexting involved girls, although there were also cases of boys who had been sent unwanted sexual images and who felt vulnerable or uncomfortable as a result.
- Many of the children and young people counselled had sent messages to relationship partners or online contacts they believed they could trust. After sharing pictures, they experienced a lack of control and fear that they would be shown to other people, leading them to regret what had happened.
- Non-consensual sharing of sexts with others had severe impacts on young people. They were often bullied and ridiculed by peers because of this, and were extremely distressed or suicidal as a result.

Childline (NSPCC 2016a) quotes the following:

> "I did something and I don't know what to do about it. I was playing dares with a boy from my school then he dared me to send nudes and I did. I feel ashamed and embarrassed and I don't know why I did it. Now I have fallen out with him he has sent the photo to everyone all over Instagram and Facebook and Snapchat and I keep getting abused at school and online saying I'm rotten and a slag. I can't tell my parents because I know they will react badly towards this. I just want it to stop!" (Girl, 12 years old)

> "I have been chatting to a girl from school online. She showed me inappropriate pictures of herself. I felt really uncomfortable with it and I am scared I will get into trouble. I told her how it made me feel but she didn't listen and kept sending me more. She laughed at me and called me names and now everyone at school thinks there is something wrong with me and says mean things." (Boy, 14 years old)

6.1.3 Experiences and gendered dimensions

Qualitative research is also important in developing an understanding of children and young people's perceptions and experiences of sexting. An exploratory qualitative study examining these issues and their peer-related contexts was conducted by Ringrose et al. (2012).[21] The key findings of the study were:

- Sexting consists of a variety of activities that can be motivated by sexual pleasure.
- However, there was evidence of the involvement of coercion, harassment and physical violence for some children and young people, which is consistent with the results of the study by Wood et al. (2015).
- There was evidence of a double standard in which girls felt pressured by boys to send sexts, but both judged girls who engaged in the behaviour negatively. Similar judgements were not made of boys who engaged in the behaviour, although they risked peer exclusion if they did not produce and circulate images of themselves.
- This reflects the shaping of sexting behaviours by the gender dynamics and norms of the peer group, as well as wider cultural influences.

This is consistent with the results of the Children's Media Lives Year 2 study (Ofcom, 2016b). This qualitative research examined gender differences in the relationship between social media, social pressure and Identity. The study found that:

[21] Single-sex focus group interviews were conducted with 35 young people from diverse ethnic and SES backgrounds in Years 8 and 10 in two inner-city schools in London. An online ethnography was also conducted with 31 participants, from which a further 22 students were selected for individual interviews.

- Girls reported experiencing high levels of physical and social scrutiny on social media. This was reflected in the described importance of receiving 'likes' and positive comments about their selfies and identity online.
- Boys were less frequent posters of selfies, with participants describing pressures to act 'tough' or being more 'laddish' on social media than they would offline.
- These results are related to the gendered perceptions of the appropriateness of sexting behaviour and unauthorised sharing, as well as the associated judgements of those involved, described above and identified in other European qualitative research (Milnes et al., 2015; van Royen, Vandebosch, & Poels, 2015).

6.1.4 Sexting and intimate partner violence (IPV)

The gender dynamics of sexting have also been examined in relation to the role of coercion within the context of young people's relationships. Wood et al. (2015), using data from STIR (n.d.), also examined the relationship between offline and online intimate partner violence (IPV), and the sending and receiving of sexual images. The results indicated that:

- Experiences of online and offline IPV victimisation increased the likelihood of young people sending and receiving sexual images.
- Both boys and girls who were a victim of online IPV were approximately twice as likely to have sent their partner a sexual image compared to those who were not (see Table 5).

Table 5: Proportion of the sample who sent a sexual image by gender and experience of online IPV

	Sent a sexual image		
	Female % (*N*)	**Male % (*N*)**	**Total % (*N*)**
Experience of online IPV	65 (124)	50 (39)	58 (163)
No experience of online IPV	24 (50)	26 (61)	25 (111)

Base: Young people aged 14-17 in England in a relationship who sent a sexual image (*N*=274).
Source: Wood et al. (2015)

This suggests that coercive sexting and threats or actual sharing of images may be part of a wider pattern of IPV in the lives of some children and young people. The intersection of sexting and IPV requires further empirical investigation in order to inform the development of targeted interventions that address this issue.

6.1.5 Parental concerns

Facts International conducted a survey on behalf of NSPCC[22] through an online questionnaire with 1,000 parents and carers examining their concerns about sexting. The key findings were:

- 73% of parents felt that sexting is always harmful and 37% were concerned about their child engaging in the behaviour in the future

[22] These results were reported by the NSPCC in Research Highlight #96 produced by the NSPCC for the UKCCIS Evidence Group, available at www.saferinternet.org.uk/downloads/Research_Highlights/UKCCIS_RH96_Young_People_and_Sexting_NSPCC_Research.pdf

- many parents are unclear about the law around sexting. For example, half of parents did not know that it is illegal for a child to create a sexual image of themselves, and 28% were unaware that it is illegal for them to send such an image to a peer
- 86% of parents indicated that they would seek help if they discovered that their child had sent a sexual image to another young person and been shared online. However, only 50% felt confident that they could access appropriate support in such a situation
- 42% of the sample had spoken to their child about sexting at least once, with 19% never intending to discuss this issue
- 83% and 84% of the sample respectively had never received or looked for information about sexting. However, 50% indicated an interest in learning more about the issue through schools and online resources
- preferred topics are healthy relationships and associated pressures on young people, as well as how they feel about sexting, and guidance on how to start related conversations.

These results suggest that sexting is a significant concern for parents, and the need for further promotion of existing educational resources and/or development of new initiatives is appropriate. Some of these concerns relate to the legal aspects of children and young people engaging in this behaviour, as discussed below.

6.1.6 Safeguarding and legal contexts

Concerns have been raised by different stakeholders about the safeguarding and legal dimensions of children and young people engaging in sexting given that the production and dissemination of sexual images of those aged under 18 is illegal in the UK. As a result, UKCCIS, in consultation with the NSPCC and other relevant stakeholders, published non-statutory guidance for schools related to responding to incidents of sexting by under-18s (UKCCIS, 2016) (c.f. Outcome 21).[23] Over 200 organisations were involved in creating the guidance, including the government and the Department for Education (DfE), children's charities, the UK Safer Internet Centre, the Child Exploitation & Online Protection Centre (CEOP), the police and teachers' groups. The guidance indicates that although sharing sexual images of themselves is illegal and risky, it is often the result of curiosity and exploration. The guidance aims to ensure that children are diverted from the criminal justice system.

The College of Policing[24] and the National Institute for Health and Care Excellence (NICE)[25] have also recently produced guidance on sexting. This includes advice to police forces on how to deal with cases where children have consensually shared indecent images with each other, and encourages officers investigating these incidents to consider if a criminal justice response is warranted. It is suggested that as first responders, safer school officers or neighbourhood teams might be able to provide a more proportionate response. However, where officers suspect the presence of exploitation, coercion, a profit motive or adults as perpetrators in the creation of the images, the case will still require a full criminal investigative response.

6.2 Online sexual harassment

The gendered nature of sexting, and the potentially negative psychological and social consequences of engaging in the activity, have also been linked to the experience of online sexual harassment, particularly for girls. This involves a number of different behaviours, including gender harassment (e.g., non-consensual sharing of sexual images to harass or embarrass, use of sexual

[23] Outcome 21 is new Outcome Code launched by the Home Office to help formalise the discretion available to the police when handling crimes such as youth-produced sexual imagery.

[24] See www.college.police.uk/News/College-news/Pages/Sexting-briefing-note.aspx

[25] See www.nhs.uk/news/2016/09September/Pages/NICE-issues-new-guidelines-on-sexting-in-teens.aspx

language or insults in comments), unwanted sexual attention and sexual coercion (van Royen et al., 2015).

There is a general lack of empirical evidence about this area of online victimisation. Although it can be conceptualised as part of cyberbullying and online harassment more generally, it has specific gendered aspects that make it a distinct form of online victimisation.

6.2.1 Offline sexual harassment

The available UK evidence is small and generally focused on the prevalence of offline sexual harassment among children and young people. This suggests such experiences are common for girls and young women, with a study by Girlguiding UK (2014) finding that 59% of girls and women aged 13-21 reported being harassed at school or college in the previous year.

Qualitative research also suggests the widespread nature of sexual harassment and its acceptance by many children and young people as a normal part of everyday life, a perception that acts as a barrier to recognition that the behaviour is problematic and subsequent reporting (Milnes et al., 2015). The young people in this study also highlighted the role of the online environment and the gendered nature of sexting in facilitating sexual bullying, consistent with the research evidence reviewed earlier (e.g., Ringrose et al., 2012).

6.2.2 Online sexual harassment

Based on this evidence, it is likely that similar patterns of sexual harassment will be reproduced in the online environment and interaction among children and young people. This is consistent with the results of a European qualitative research study addressing this issue (van Royen et al., 2015):

- A focus group study of Belgian adolescents aged 12-18 found that personally targeted gender harassment (e.g., slut-shaming, homophobic comments) was viewed as normalised, with participants also mentioning non-consensual sharing of sexual images, use of insulting language and frequent unwanted sexual attention from adults as forms of bullying.
- These behaviours are more frequently experienced by girls and young women, although boys report the normalisation of homophobic bullying online.

6.3 Current knowledge gaps

The review of the available evidence has identified the following areas requiring further research in order to develop greater understanding of the prevalence, experiences and consequences of sexting and sexual harassment among young people in the UK:

- variations in prevalence by age and gender
- gendered perceptions, dynamics and impacts
- relationship contexts of sexual content production and sharing, both positive and negative.

We also need more research on:

- prevalence, dynamics and impacts of online sexual harassment in different groups of children and young people (e.g., age, gender and gender identity, sexual orientation)
- the relationship between online (and offline) sexual harassment, physical violence and sexual exploitation by peers and adults

- effective educational resources for all stakeholders to challenge this behaviour and its perceived normalisation in the online environment.

6.4 Summary

The available evidence on sexting suggests that:

- The majority of children and young people do not engage in sexting.
- It is unclear whether claims that it is a normalised adolescent behaviour are justified.
- The prevalence of sexting is higher for older adolescents.
- Many children and young people who engage in the behaviour do so in the context of romantic relationships.
- Commonly reported motivations are to flirt and in response to partner requests in relationships.
- Many children and young people report that this is a positive activity/experience.
- However, there is evidence that some girls and boys experience pressure and coercion to engage in this behaviour within their relationships.
- There is also evidence that children and young people who experience IPV are more likely to engage in the production and sharing of sexual images in the context of a coercive relationship.
- Sexting occurs in a gendered context in which girls may feel pressurised to send sexual images and boys may share/post images to maintain social status in peer networks.
- The wider sharing of sexting imagery has significant psychological and social impacts on children and young people.
- Although engaging in this behaviour is illegal in the UK, current UKCCIS guidance recommends that incidents which are reported to schools should be generally addressed as a safeguarding issue rather than a criminal activity requiring involvement of the police.
- Parents are concerned over the prevalence and impacts of sexting, and would benefit from further educational resources addressing this issue.

As for sexual harassment, the evidence suggests that:

- Many children and young people experience sexual harassment and bullying in the online and offline environment.
- It exists on a continuum from use of gendered and sexual insults, unauthorised sharing of images, through to threats and coercion and sexual violence.
- There are gendered patterns of engaging with and being targeted by this behaviour that reflect wider cultural gender dynamics and norms.
- These behaviours are normalised and are seen as acceptable behaviour or ‘banter’ among boys; girls feel unable to effectively challenge such beliefs.
- Boys also experience online sexual harassment, particularly bullying around sexual orientation.

7. Pornography

7.1 Definition and prevalence rates

There have been several recent reports covering young people's intentional or unintentional access to pornography, and the emotions and attitudes that such viewing can elicit. Pornography can be defined as:

> … images and films of people having sex or behaving sexually online. This includes semi-naked and naked images and films of people that you may have viewed or downloaded from the internet, or that someone else shared with you directly, or showed to you on their phone or computer. (Martellozzo et al., 2016, p. 16)

One of the most significant UK studies conducted to date by Martellozzo et al. (2016) on behalf of the NSPCC and the Office of the Children's Commissioner suggests that:

- more boys view online pornography, through choice, than girls
- at 11, the majority of children had not seen online pornography
- by 15, children were more likely than not to have seen online pornography
- children were as likely to stumble across pornography via a 'pop-up' as to search for it deliberately or be shown it by other people.

One of the largest systematic reviews of empirical research (published in peer-reviewed journals between 1995 and 2015) was conducted by Peter & Valkenburg (2016) who examined the prevalence, predictors and implications of adolescents' use of pornography, and concluded that:

- adolescents consume pornography, but it is difficult to provide stable prevalence rates as figures vary greatly from study to study
- the typical adolescent pornography user is a male, pubertally more advanced, sensation-seeker with weak or troubled family relations
- there was a relationship between pornography, sexual attitudes of young people and some sexual behaviours, but causality was not always clear.

Horvath et al.'s (2013) cross-national rapid evidence assessment on the effects that exposure to pornography have on children and young people's sexual beliefs also found widely varying prevalence figures, for example:

- exposure and access rates for boys ranged from 83 to 100%
- reported rates for girls ranged from 45 to 80%.

A recent Net Children Go Mobile report stated that 17% of 516 UK 9- to 16-year-olds have seen sexual images online or offline within the last year, a figure that is lower than the 28% found across Europe, and lower than the figure of 24% reported in 2010 for the UK (Livingstone et al., 2014a). How children are exposed to online pornography can be seen below.

Table 6: How children are exposed to online pornography, by age

%	Age				All
	9-10	11-12	13-14	15-16	
In a magazine or book	0	0	6	12	5
On television, film	1	0	7	15	6
On a video sharing platform	1	0	2	13	4
On a photo sharing platform	0	0	3	9	4
By pop-ups on the internet	0	3	11	4	5
On a SNS	0	4	7	13	7
By instant messaging	0	0	1	11	3
In a chatroom	0	0	1	0	0
By email	0	0	0	0	0
On a gaming website	0	0	0	0	0

NCGM: Q36: If you have seen images of this kind, how did it happen? (multiple responses allowed)
Base: All children who use the internet.
Source: Mascheroni & Ólafsson (2014)

Research conducted by the NSPCC with a non-random sample of 1,700 children aged 11-18 (2016d) indicates that children were most likely to see inappropriate content on:

- Dating sites (70% of children saw inappropriate content on the two sites reviewed, Tinder and MeetMe)
  - 57% saw sexual content
  - 50% saw 'adult' content
- Photo/image sharing sites (51% of children saw inappropriate content)
  - 35% saw bullying behaviours (the worst offenders were Yik Yak, ASK.fm)
  - 26% saw sexual, adult and violence/hatred content (the worst offenders were MeowChat, Tumblr)
- Content sharing sites (50% of children saw inappropriate content)
  - 33% saw bullying behaviour
  - 31% saw violence/hatred content
- Messaging sites (44% of children saw inappropriate content)
  - 27% saw bullying behaviour
  - 24% saw violence/hatred
- Video chat (42% of children saw inappropriate content)
  - 28% saw bullying behaviour
  - 22% saw sexual behaviour (the worst offenders were Omegle, MeowChat and Chatroulette)
- Voice calls (33% of children saw inappropriate content)
  - 22% saw bullying behaviour
  - 18% saw sexual content
- Gaming (29% of children saw inappropriate content)
  - 21% saw violence and hatred
  - 16% saw bullying behaviour

Children were most likely to say that the following groups of sites were most 'risky':

- Dating – 73%
- Photo or image sharing – 38%
- Video chat – 34%

7.2 Intentional vs. unintentional exposure

Research findings suggest more children are more likely to report unintentional rather than intentional viewing of pornography. This may happen through a number of different ways such as pop-ups, misleadingly named websites or advertising on illegal streaming sites (for more information, see Livingstone & Smith, 2014; Watters, 2014).

A report considering issues discussed in Childline counselling sessions states that accessing pornography at school was a growing problem. Young people reported fellow pupils having pornographic images on their phone and being forced into looking at them or to face being ridiculed for refusing (NSPCC, 2016b):

> "I have been bullied into watching pornographic videos by people at school, which makes me feel sick. One showed a woman being raped, it was so upsetting. They have been bullying me for a while now and I am feeling sad, depressed and sometimes have suicidal thoughts." (Boy, 13 years old)

This is an important point as it has been found in previous research that in a study by Ybarra and Mitchell (2005), young people who reported unintentional online exposure to pornographic images were also two-and-a-half times more likely to report intentional exposure. The consequences of getting introduced to pornography at a young age can be severe, with some reporting to Childline that they stayed up so late watching pornography that they struggled to concentrate at school the following day because they were so tired. Lack of sleep was resulting in problems concentrating and mood swings, and their schoolwork was suffering. Other children felt that exposure to pornography was affecting their relationships (NSPCC, 2016b).

7.3 Attitudes to online pornography

Gender differences exist regarding both exposure and attitudes towards pornography (Livingstone & Mason, 2015). Exposure to pornography impacts children's sexual attitudes, expectations and beliefs. Boys may view pornography in a more positive light, claiming it to be an educational tool, while girls see it as unwelcoming and socially distasteful (Horvath et al., 2013).

In a survey of 500 18-year-olds conducted by the Institute for Public Policy Research (Parker, 2014):

- more young men (45%) than young women (29%) agree that 'pornography helps young people learn about sex'
- only half as many young men (21%) as young women (40%) strongly agree that 'pornography leads to unrealistic attitudes to sex'
- half as many young men (18%) as young women (37%) strongly agree that 'pornography encourages society to view women as sex objects'.

Peter and Valkenburg's (2016) comprehensive review also suggested that pornography use is associated with more permissive sexual attitudes and stronger gender-stereotypical sexual beliefs. Pornography use among adolescents is also related to the incidence of sexual intercourse, greater experience with casual sex and more sexual aggression, in terms of perpetration and victimisation.

The results found are consistent over time and cross-culturally. For example, in Horvath et al.'s (2013) cross-national rapid evidence assessment on the effects that exposure to pornography has on children and young people's sexual beliefs, similar risks were discussed. Within this study, pornography has been linked to:

- unrealistic attitudes about sex
- maladaptive attitudes about relationships
- more sexually permissive attitudes
- greater acceptance of casual sex
- beliefs that women are sex objects
- more frequent thoughts about sex
- sexual uncertainty.

7.4 Risk and harm

In addition to the impact of viewing pornography on young people's general sexual behaviour and sexual risk taking, there is also evidence that viewing extreme pornography may be associated with sexually deviant/coercive behaviour.

A recent report by Stanley et al. (2016) supports the findings above, and that negative gender attitudes were also positively associated with sexual coercion among boys. Results from a large survey of 4,564 young people aged 14-17 in five European countries (including the UK) highlights the relationship between online pornography viewing, sexual coercion and abuse, and sexting. In all five countries examined boys who regularly watched online pornography were significantly more likely to hold negative gender attitudes:

- Both regularly watching pornography (OR = 2.2) and sending (OR = 2.8) or receiving (OR = 1.9) sexual images or messages was associated with an increased probability of being a perpetrator of sexual coercion.[26]

While it is beyond the scope of the current review to cover this topic in greater detail, information on the topic can be found in numerous reports such as Belton & Hollis' report (2016), who conduct a review of international research.

7.5 Children's concerns

The apprehensions regarding pornography are not lost on young people themselves. In the EU Kids Online survey of 2010, 10,000 children aged 9-16 described what upset children their age online. Pornography topped the list of online content-related concerns (Livingstone et al., 2014b). There was a large increase in children and young people contacting Childline about viewing sexually explicit images – up 60% from 2014/15.[27]

Parker's (2014) survey results showed that:

- overall 70% felt that pornography could have a damaging impact on young people's views of sex and relationships
- 66% of young women and 49% of young men agree that 'it would be easier growing up if pornography was less easy to access for young people'

[26] An *odds ratio* (OR) is a measure of association between an exposure and an outcome. The OR represents the *odds* that an outcome will occur given a particular exposure.

[27] While numbers of young people who have contacted Childline regarding viewing sexually explicit images are up 60%, numbers are still low – 844 out of 11,000 counselling sessions in 2015/16.

- overall, two thirds (66%) believe that 'people are too casual about sex and relationships'
- 77% of young women state that 'pornography has led to pressure on girls or young women to look a certain way'
- 75% of young women believe 'pornography has led to pressure on girls and young women to act a certain way'.

7.6 Interventions

Within Martellozzo et al.'s (2016) study, focus group participants suggested that unhealthy attitudes towards women, and sexual relationships that can arise from exposure to online pornography, may be negated by introducing formal school education on the issues surrounding online pornography. Children and young people who are educated about online pornography during sex education or PSHE (Personal, Social and Health Education) classes may be less likely to be negatively influenced by online pornography than those who have not had lessons on the topic. PSHE classes may be associated with greater awareness of the issues surrounding pornography – along with other risks. The study also allowed participants to express how they felt interventions should be approached. Interventions should:

- provide safe, secure online engagement
- be private and not entirely online
- be gender and age-appropriate
- help teachers and/or specialised staff to co-create learning with young people
- support young people in ways that acknowledge their social sexual development and perceived peer group expectations.

7.7 Summary and evidence gaps

The impact of pornography on children can be summarised as follows:

- Exposure and access rates are different for boys and girls (83% to 100% vs. 45% to 80%).
- Gender differences exist in attitudes towards pornography.
- Exposure to pornography has adverse effects on children and young people's sexual beliefs.
- There is evidence that extreme porn may be associated with sexually deviant/coercive behaviour.
- Pornography is the top content-related concern for children.
- Sex education classes can help counter the negative effects of pornography.
- It is important to address the messages that boys take from viewing pornography, and what their expectations are for the girls with whom they interact.
- Similarly, there needs to be further examination of the messages that girls take from pornography, and how they may be being influenced within potential or actual sexual relationships.
- More research is needed that looks more directly at the effects of young people's viewing of pornography on their development and relationships.
- There needs to be more research on the impact of violent pornography on young people's behaviour.

8. Grooming, child sexual abuse and exploitation

8.1 Prevalence and definition of grooming and child sexual exploitation

Although some recent research has been conducted that explores online offender behaviour and children's experience of online abuse (Davidson et al., 2016; Webster, Davidson, & Bifulco, 2014; Whittle, Hamilton-Giachristsis, & Beech, 2014), we still have limited knowledge about the nature of sexual crimes against children mediated through information and communication technologies (ICT), those who perpetrate them, and the impact of these crimes on children. It is clear from research with practitioners (Palmer, 2015) and young people who have been abused online (Quayle, Jonsson, & Lööf, 2012) that online grooming is rarely disclosed by the victims who may be in fear of the perpetrator or who may feel that they are in a relationship with the perpetrator; consequently, research and official statistics reflect only reported offences and experiences.

We have even less knowledge about the nature of the link between online abuse and contact offending, although some recent good international research has been undertaken in this area (see, for example, Seto, 2016). Given the lack of research in this area, only key studies are reported, some of which were published before 2012 and some of which are international in focus.

This section focuses on adult grooming of children and young people. 'Grooming' refers to a process of socialisation through which an adult engages with and manipulates a child or young person for the purpose of online sexual abuse (which may include offline aspects). Studies that have explored the prevalence of 'sexual solicitation' or 'grooming' (i.e., an adult encouraging a child to talk or do something sexual or to share personal sexual information) in the general child population have produced a variety of results depending on the research sample characteristics and the method employed. Estimating prevalence is problematic given that the Home Office has only recently begun to collect criminal justice data on reported online child sexual abuse cases in 2016, and self-report surveys are reliant on the willingness of young people to disclose abuse.

Key recent studies suggest that:

- the police encounter online child sexual abuse cases on a weekly basis (Davidson et al., 2016)
- 7.1% of the adult participants in a national survey had communicated about a sexual topic with unknown adolescents and 0.5% with children (Bergen et al., 2014)
- 9% of adolescents aged 10-17 reported having experienced unwanted sexual solicitation in a large US survey (Jones, Mitchell, & Finkelhor, 2012)
- an analysis of reports and associated texts from an online child sexual exploitation tipline in Canada indicated that most online victims are girls, and the mean age of victims is 13.5 years.

In comparison, other recent research conducted by Davidson et al. (2016) in four EU countries that included national police and retrospective children and young people's victimisation surveys suggests that most young people (70%) never received requests for sexual behaviour online during their formative years, and 79% were never asked to meet to engage in sexual activities (see Table 7 below).

***Table 7: Being invited to act sexually online*[28]**

Invited to act sexually online	Often	Sometimes	Rarely	Never	Total
	N (%)	*N* (%)	*N* (%)	*N* (%)	*N* (%)
Ask for sexual information about yourself	51 (4)	213 (19)	220 (19)	658 (58)	1,142 (100)
Ask to do something sexual	36 (3)	127 (11)	185 (16)	794 (70)	1,142 (100)
Ask for a sexual photo/video of yourself	51 (4)	151 (13)	185 (16)	755 (66)	1,142 (100)
Meet up to engage in sexual activities	23 (2)	78 (7)	137 (12)	903 (79)	1,141 (100)

Source: Davidson et al. (2016)

Although there is no certainty regarding the incidence of 'grooming', it is a legal concept in many countries, and the EU directive on combating child sexual abuse and sexual exploitation (including online grooming) and the collection, possession and distribution of child indecent imagery introduced in 2011 sought to curb the exploitation of children on the internet and required implementation by member states (European Parliament, 2011). The grooming clause was first introduced to English law in the Sexual Offences Act 2003 and was updated in Section 67 of the Serious Crime Act 2015 (sexual communication with a child).

The Home Office defines child sexual exploitation as follows (DfE, 2017, p. 5):

> Child sexual exploitation is a form of child sexual abuse. It occurs where an individual or group takes advantage of an imbalance of power to coerce, manipulate or deceive a child or young person under the age of 18 into sexual activity in exchange for (a) something the victim needs or wants, and/or (b) the financial advantage or increased status of the perpetrator or facilitator. The victim may have been sexually exploited even if the sexual activity appears consensual. Child sexual exploitation does not always involve physical contact; it can also occur through the use of technology.

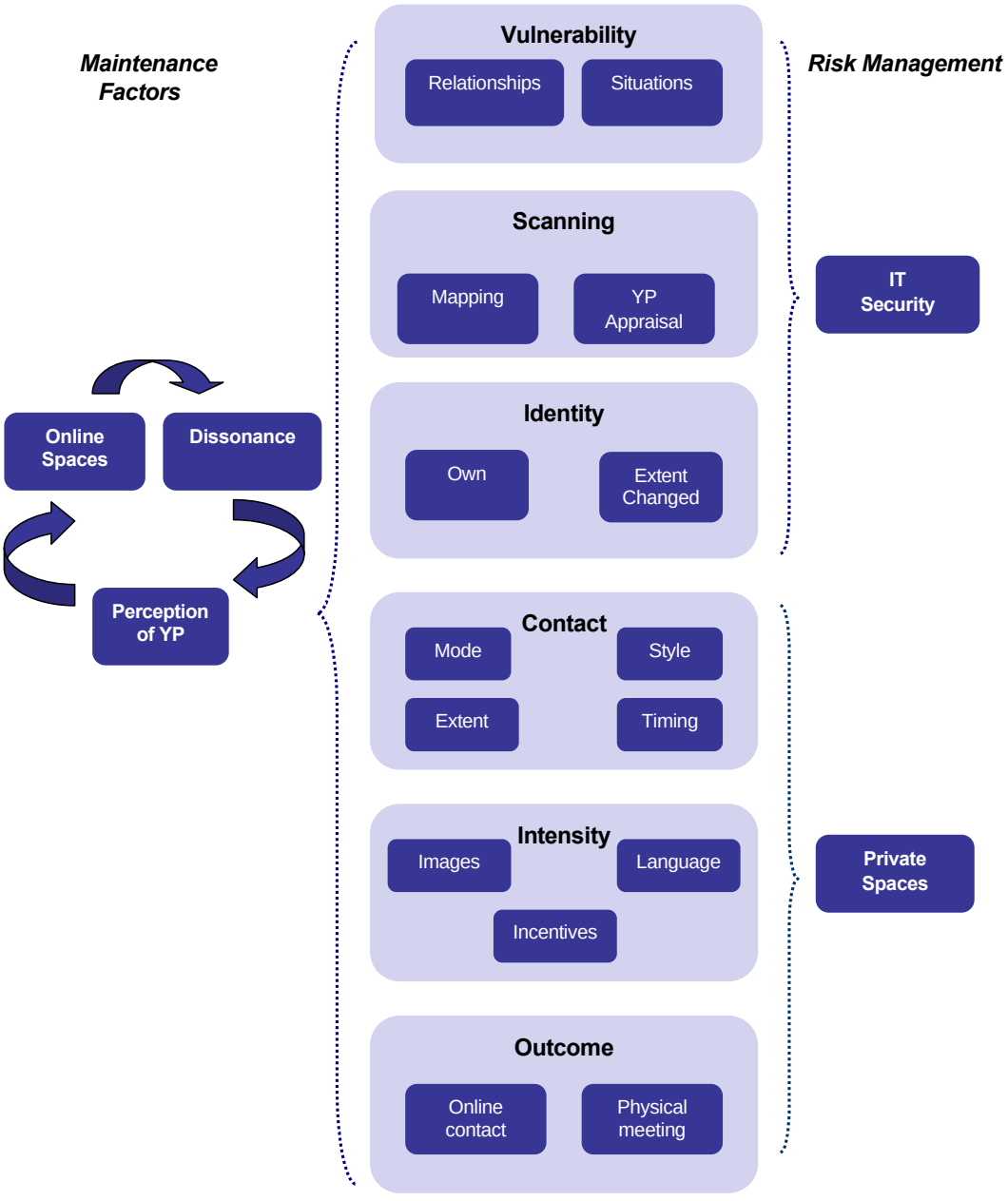
This form of abuse clearly overlaps with child sexual abuse and grooming, but the term is not widely recognised internationally, and research to date has not yet distinguished between online child sexual exploitation and other forms of online child sexual abuse. There is a need for future research to focus on this issue.

[28] The retrospective young person survey asked young adults (18-25) about their experiences between the ages of 12-16. The sample consisted of 1,166 respondents across three countries: England (*N*=340), Ireland (*N*=529) and Italy (*N*=297). The average age was 21.23 years (SD = 2.15, range 18-25). The gender breakdown was disproportionate in the three countries, but the majority were females (Ireland: female = 344, male = 185; Italy: female = 222, male = 75 and England: female = 271, male = 69) (Φ=0.14, *p*=<0.001).

8.2 The grooming process

Contact offences often occur as a result of a grooming process, although grooming doesn't always result in a contact offence; some offenders simply seek online gratification. Webster et al. (2012) produced one of the first online grooming process models. They conducted a study consisting of a literature review, a review of case files, interviews with stakeholders and interviews with convicted offenders. The study concentrates on the UK, Norway, Italy and Belgium. The model proposes six phases: vulnerability, scanning, identity, contact, intensity and outcome. Two further elements, risk management and offence maintenance, support the grooming process. Figure 20 illustrates the interrelationships of the different phases within the grooming model.

Figure 20: Model of online grooming



Source: Webster, Davidson and Bifulco (2014). YP = young person.

Elzinga, Wolff and Poelmans (2012) provide a similar model of the grooming process, adding strength to the model proposed by Webster et al. (2012). Whittle, Hamilton-Giachritsis and Beech (2014) found participants who had been sexually abused online and/or offline had a range of grooming experiences, including:

- manipulation
- deception
- regular/intense contact
- secrecy
- sexualisation
- kindness and flattery
- erratic temperament and nastiness
- simultaneous grooming of those close to the victim.

The findings are similar to themes originally identified by Webster et al. (2012) and other earlier literature in this area (see, for example, Quayle, Jonsson, & Lööf, 2012). These tactics are likely to make the victims feel familiarity, love, trust, increased confidence, emotional support and excitement, but also a lack of control, confusion, reliance on the offender and distancing from family members. Once an individual is 'enmeshed' in the relationship with an offender they are more likely to endure negative feelings associated with the grooming but equally develop a bond with the offender.

Recently, a communication model for grooming discourse was formulated by Lorenzo-Dus, Izura and Pérez-Tattam (2016). This model is based on analysis of a large data set (approximately 75,000 words) of online groomer chatlogs. Using various processes such as desensitisation, reverse psychology, reframing and isolation among others, results suggest that there are four main strategies used by groomers when communicating. These included:

1. *Deceptive trust development:* groomers disguise their main intention to engage a child in sexual behaviour by cultivating a personal and friendly relationship.
2. *Sexual gratification:* groomers prepare the child to accept offline sexual contact and to engage in online sexual activities.
3. *Compliance testing:* groomers gauge the extent to which the child is an actual minor and will agree to engage in the sexual activities proposed.
4. *Isolation:* groomers develop the secrecy of their intended relationship with the child, including efforts to avoid discovery by the child's support network.

The researchers concluded that victim–offender relationships are as varied and complex as the individuals involved, and although the processes may differentiate between 'dyads', the use of cognitive distortions on the part of the offenders and the emotional effect the entire process has on the victims is constant. In short, research suggests that online grooming is varied, cyclical and occurs in a non-linear process.

8.3 The impact on children and seeking support

It is clear that the consequences of sexual grooming can be and often are devastating for the child, potentially impacting on their lives and future relationships (Quayle, Jonsson, & Lööf, 2012). However, the impact will vary depending on the nature and severity of the abuse and possibly the extent to which contact abuse is involved. Nevertheless, Whittle, Hamilton-Giachritsis and Beech's (2014) study with young people experiencing abuse concludes that:

> There is no evidence in this study to suggest that those who were also abused offline experienced greater negative impact of abuse than those who were abused online only.

> This supports emerging research. Instead, the negative effects of abuse appear to be correlated with the risk and protective factors impacting upon the individual before the onset of the grooming. (Whittle, Hamilton-Giachritsis, & Beech 2014, p. 67)

This finding is supported by Webster, Davidson and Bifulco (2014) and Webster et al. (2012), who suggest that children who are vulnerable offline may also be vulnerable online. However, Whittle, Hamilton-Giachritsis and Beech's work was based on only a small number of qualitative interviews, and more research is needed to validate this finding. According to findings by Gunnell et al. (2014), victims of grooming and online child sexual abuse often report long-term psychological issues as well as suicide ideation and attempts. It is clear that the impact of the initial and early online grooming approach on children will vary: some children will become distressed (Priebe, Mitchell, & Finkelhor, 2013), some will take action to block or report the approach (Priebe, Mitchell, & Finkelhor, 2013; Webster, Davidson, & Bifulco, 2014), some will ignore the approach, and some will engage with the sender (Webster et al., 2012).

Research indicates that some children may confide in others or report what has happened; however, a significant number of young people do not confide in parents or teachers for a number of reasons – they consider the behaviour normal, they feel uncomfortable talking to parents or they fear the removal of their electronic devices as a result of their parents discovering (Priebe, Mitchell, & Finkelhor, 2013). Understanding whom children are likely to confide in when distressed about online sexual solicitation is vital as there has been limited research conducted in this area. As part of their research, Mitchell et al. (2013) examined children and young people's disclosure of online solicitation incidents, and found that 53% of solicitations were disclosed to a trusted individual. Most participants disclosed information to a friend (37%) or parent/guardian (19%). Very few incidents were reported to a teacher or a higher authority such as law enforcement.
Davidson et al.'s (2016) research explored children and young people's informal and formal help-seeking behaviour following an experience of online victimisation in childhood (see Table 8). In keeping with the Priebe, Mitchell and Finkelhor. (2013) study, this research suggests that children rarely seek help from authority figures and are more likely to confide in friends (33%) than their parents (4%).

Table 8: Rates of informal and formal help-seeking behaviour

Informal help-seeking behaviour				Formal help-seeking behaviour			
Question asked	Yes	No	Total	**Question asked**	Yes	No	Total
	N (%)	*N* (%)	*N* (%)		*N* (%)	*N* (%)	*N* (%)
I told my mother or father	27 (4)	568 (96)	595 (100)	**I called a helpline**	1 (0)	589 (100)	600 (100)
I told my brother or sister	18 (3)	574 (97)	592 (100)	**I told a teacher**	3 (1)	587 (99)	590 (100)
I told a friend	218(33)	446 (67)	664 (100)	**I told someone whose job it is to help (i.e., police, social worker)**	7 (1)	586 (99)	593 (100)
I told my boyfriend/ girlfriend at that time	42 (7)	558 (93)	600 (100)	**I used an online reporting mechanism**	13 (2)	579 (98)	592 (100)
I told another adult I trust	5 (1)	584 (99)	589 (100)				
I told someone else	26 (4)	564 (96)	590 (100)				
***N* = Number of participants.**							

Source: Davidson et al. (2016)

8.4 Indecent images of children

8.4.1 Scale and nature of the problem

Indecent images involve the creation, distribution and collection of sexually explicit images and videos of children and young people otherwise referred to in the recent literature as ‘child abuse material’ (CAM) (Aiken, Moran, & Berry, 2011). The increase in the number of indecent images of children in the hidden web poses huge challenges to both industry and criminal justice agencies alike. The National Centre for Missing and Exploited Children (NCMEC) reported that throughout January 2015 they had analysed more than 132 million images and videos depicting CAM using identification software (NCMEC, 2015).

The largest and most recent UK study was conducted by Quayle, Goren Svedin and Jonsson (2017), and this analysis of 687 images from the UK International Child Sexual Exploitation Database (UK ICSE DB) shows an increase of identified victims from 2006-15. Almost two thirds of the victims were girls and the vast majority were white. It has been suggested that requests for sexual pictures from minors through mobile phones and webcams is now pervasive and possibly plays a central role in the grooming process (Quayle & Newman, 2016). In this review of grooming incidents reported to Canada’s tipline dealing with the online sexual exploitation of children (www.cybertip.ca/app/en/), 155 of the 166 reports (93.8%) examined found specific requests by suspects for pictures from children. There is very little recent UK research in this area and this represents a significant gap. Please note that peer-to-peer indecent images are discussed in the section on ‘sexting’ (see Section 6.1.6).

Childline data provide an insight into the sorts of issues children who are upset, scared or worried are seeking support and advice about. The impact that viewing such images has on children emerged during a 2015/16 review of 68 counselling sessions where a young person said they had viewed illegal CAM online. Children interviewed indicated that:

- images had mainly been accessed unintentionally (e.g., via a pop-up/unknown link)
- young people were worried about being in trouble with the police or not being believed that they were exposed to it unintentionally
- they were suffering from a lack of sleep and/or having anxiety attacks as a result (NSPCC, 2016c).

8.4.2 Responding to children sexually abused online

Research conducted by Bond, Agnew and Phippen (2014) in conjunction with the Marie Collins Foundation has suggested that practitioners working with children and young people are ill-equipped to respond to the needs of child victims of online sexual abuse. Further:

- 70% of the respondents from Health, Education and Children's Services stated that they had not received training in online risk assessment, and 96.5% said they would value such training
- 81.1% of the respondents said they had received no training in assisting children in their recovery from online abuse, and 94% stated that they would value such training.

This work points to the need for a nationally recognised training programme for those working with children harmed through online abuse. The research aimed to explore practitioners' training needs, and found that the current response is ad hoc and not informed by research evidence or best practice. Davidson et al.'s (2016) recent EC-funded research conducted with the police concluded that much greater coordinated and standardised collaboration is needed between industry and law enforcement in the prevention and investigation of online child sexual abuse.

8.5 Summary

There is very little large-scale UK research exploring the sexual abuse and exploitation of children online, and the EU has funded most of this research. The main findings are as follows:

- It is difficult to estimate the prevalence of online grooming in the UK due to the unreliability of official estimates that have only recently begun to include online child abuse offence categories, and due to the absence of large-scale self-report studies addressing this issue.
- EU and US surveys suggest online child grooming or sexual solicitation rates of 7-9%; a recent national survey of police officers in England suggests that online child sexual abuse cases are encountered on a weekly basis.
- Recent research indicates that online grooming behaviour is varied, cyclical and occurs in a non-linear process.
- Research with child victims of online grooming has demonstrated that the impact on them is very often devastating. It is also clear that children are unlikely to confide in parents or teachers or to seek support about their experiences.
- There is no UK research exploring the experience of children appearing in indecent images. Analysis of images suggests that requests for sexual pictures through mobile phones and webcams are now pervasive and possibly play a central role in the grooming process.

9. Online radicalisation

Radicalisation is defined by Geeraerts (2012, p. 26) as:

> … a process whereby an individual comes to embrace values and opinions about a certain topic … that gradually become more extreme and hence start to deviate more from the normative opinions, while at the same time finding it more difficult to accept opposite opinions.

Opinions can be based on various topics such as politics, religion and philosophy among others, and in extreme cases can lead to ideological violence such as terrorism. There are many factors that have an influence on the development of ideological beliefs, and there is evidence to suggest that the internet is playing a considerable role in facilitating such processes among young people.

9.1 Prevalence

While several studies examining online radicalisation cover adult internet participation, research into the online radicalisation of young people in a UK context has been sparse (Edwards & Gribbon, 2013; von Behr et al., 2013). Additionally, few studies have attempted to quantify the regularity of these behaviours, and instead usually consist of case studies or reviews of anecdotal evidence. It should also be noted that while some research covered in this report included other extreme groups such as the far right (Edwards & Gribbon, 2013), the majority of online radicalisation research reviewed has had a focus on Islamic radicalisation.

Channel is a branch of the UK's counter-terrorism strategy and forms a major part of the Prevent strategy that provides support to individuals (including young people) who are at risk of being drawn into terrorism or extremism. Between April 2007 and the end of March 2014 Channel received a total of 1,450 referrals who were under 18 years of age at the time they were referred.[29]

The Children and Family Court Advisory and Support Service (Cafcass, 2016) also has some figures concerning radicalisation. Cafcass is a non-departmental public body set up to promote the welfare of children and families involved in family court. According to a review of Cafcass cases, over the course of six months in 2015, 10 cases involved the suspected radicalisation of the child specifically as the principal reason for the proceedings being opened.

9.2 The role of the internet and social media

As highlighted in this report, young people today have almost universal access to the internet through various devices, and one of the most popular uses of the internet among them is for social networking (Childwise, 2017). This is a fact that extremist groups are exploiting, thus making young people potentially vulnerable to harm and propaganda from Islamic and far-right extremist groups (Twitter confirmed that between mid-2015 and February 2016 it had suspended over 125,000 accounts globally that were linked to terrorists) (Corb & Grozelle, 2014; House of Commons, 2016; Mughal, 2016).

The internet is believed to facilitate the grooming of those targeted by providing uncensored messages and a sense of anonymity in what is viewed, and the grooming process may be similar to that identified in the online sexual abuse literature (Webster et al., 2012), but research is yet to confirm this. The internet also makes it easier for knowledge transfer and the dissemination of

[29] See www.npcc.police.uk/FreedomofInformation/NationalChannelReferralFigures.aspx

information to a larger audience, which provides an opportunity for self-radicalisation (whereby no contact is made with other terrorists or extremists, whether in person or virtually) (von Behr et al., 2013).

Research analysing the role of the internet in the radicalisation of 15 terrorists and extremists who were arrested in the UK found that younger offenders were significantly more likely to engage in extremist virtual learning and virtual interaction than older offenders (Gill et al., 2015).
Von Behr et al. (2013) examined the role the internet had in 15 cases of terrorism and extremism. The study was based on data drawn from a variety of sources such as evidence presented at trial, computer registries of convicted terrorists, interviews with convicted terrorists and extremists, as well as law enforcement. The study had five major findings, that the internet:

- creates more *opportunities* to become radicalised
- acts as an '*echo chamber*', a place where individuals find their ideas supported and echoed by other like-minded individuals
- *accelerates* the process of radicalisation
- allows radicalisation to occur *without physical contact*
- increases opportunities for *self-radicalisation*.

The UK's National Counter Terrorism Security Office reports that terrorist groups have harnessed the power of social media and are increasingly reaching out to young people using the web as a tool for recruitment and radicalisation.[30] In one of the most comprehensive reports on individuals arrested in the US for supporting Islamic State (ISIS) it was discovered that ISIS were proficient at directly contacting US citizens on a constant basis through social media, which helped advance the radicalisation process (Hughes & Vidano, 2015). Geeraerts (2012) states that young people are more vulnerable to online radicalisation because they are the heaviest users of the internet, and are more likely to encounter political and civic issues through the medium.

Von Knop (2007) has suggested that young people are drawn to web-based media in three ways:

- accidental exposure to content while exploring the internet for entertainment purposes.
- out of curiosity when seeking related information concerning ideology or traditions that may be associated with a radical group
- when looking for a social community with which they can identify.

9.3 Characteristics of vulnerable young people and recruiters

Recruiters can be very adept at targeting a young audience (e.g., the creation of online video games to promote extremism). Bizina and Gray (2014) state that many vulnerable young people who ended up becoming radicalised after feeling that society had rejected them found virtual networks online. There may also be an issue for some young people around identity, and an inability for parents to pass on their views about the traditional practice of religion, or to enable their children to challenge beliefs, particularly where parents lack the necessary English language skills. While speaking at the House of Commons, Baroness Shields, Minister for Internet Safety and Security, stated that children are "more technologically literate than their parents and teachers" and are particularly susceptible to online influences because they are "almost constantly connected to the digital world". She stated that the extremists who influence them are from this same social media-connected peer group.
However, it is important to note that even young people who would not usually be classified as 'vulnerable' have been found to be successfully radicalised. This was found in several cases referred to Cafcass regarding females who were reported to have no clear vulnerabilities and who

[30] See www.gov.uk/government/publications/online-radicalisation/online-radicalisation

could be described as socially and academically successful (Cafcass, 2016). Findings such as these provide evidence as to why research in the area has found it difficult to create profiles or typologies of young people at risk of radicalisation, particularly because there is little heterogeneity in terms of the education, family background, social class, income and religion of convicted perpetrators (Youth Justice Board, 2012a). Reports suggest that general indicators of vulnerability are applicable to radicalisation as follows:

- family tensions
- a sense of isolation
- migration
- distance from cultural heritage
- experience of racism or discrimination
- feeling of failure etc. (Bailey, 2015).

Research on the characteristics of young people in the UK specifically vulnerable to online radicalisation has been sparse. For a systematic review of the characteristics and behaviours of individuals vulnerable to radicalisation, please see the evidence presented by the Youth Justice Board (2012a).

9.4 Interventions

In terms of content, a specialist police unit exists in the UK called the Counter Terrorism Internet Referral Unit (CTIRU), which works to remove online content that breaches terrorist legislation. It was established in 2010 and at the start of 2016, it had removed more than 120,000 pieces of terrorist-related content. This would have included the suspension of accounts of those propagating terrorist or extremist views and the taking down of websites promoting this type of content (removal requests average 1,000 a week) (House of Commons, 2016).

In 2011, the UK government introduced the *Prevent* strategy as part of the overall counter-terrorism strategy, *CONTEST*.[31] The aim of the Prevent strategy is to reduce the threat to the UK from terrorism by recognising and intervening when there is a suspicion that people are supporting terrorism or evidence of behaviours relating to terrorism. The Prevent Duty supplies guidance for schools and childcare providers on preventing children and young people from being drawn into terrorism (DfE, 2015).

Channel forms a major part of the Prevent strategy, and provides support to individuals who are at risk of being drawn into terrorism. The programme uses a multi-agency approach to protect vulnerable people by:

- identifying individuals at risk
- assessing the nature and extent of that risk
- developing the most appropriate support plan for the individuals concerned.

Channel provides an online training module to provide awareness and information on how to identify factors that can make people vulnerable to radicalisation. The module is suitable for school staff and other front-line workers. Many children referred will not have been suitable for Channel and will have been signposted to other services more appropriate to their needs. Examples of other services include the Preventing Violent Extremism (PVE) programmes assessed by the Youth Justice Board. The Board secured resources from the Office of Security and Counter Terrorism (OSCT) to fund programmes within youth offending teams to prevent at-risk young

[31] See www.gov.uk/government/publications/2010-to-2015-government-policy-counter-terrorism/2010-to-2015-government-policy-counter-terrorism

people from becoming involved in radicalisation and violent extremism (Youth Justice Board, 2012b).

More research on youth exposure to online radicalisation is vital as once exposed to a radicalised network or group, that group can act as a catalyst, spurring the individual into violent action (Youth Justice Board, 2012a).

9.5 Summary

Regarding online radicalisation:

- There is presently a lack of research into the area of online radicalisation among young people in the UK. This is because access to extremists and primary data is difficult to achieve.
- Examining the possible influence of the internet on the radicalisation of young people is vitally important, considering the profound impact of the internet on their lives.
- The internet increases opportunities for self-radicalisation and radicalisation without physical contact.
- Terrorists have harnessed the power of social media to target vulnerable young people.
- As part of its counter-terrorism and counter-radicalisation strategy, the UK launched Prevent for its educational institutions, although its uptake was limited due to some of its controversial provisions.

10. Hacking

10.1 Definition of hacking

According to the Home Office cybercrime review, hacking involves the 'unauthorised use of, or access into, computers or network resources, which exploits identified security vulnerabilities in networks' (McGuire & Dowling, 2013, p. 5). Cyberspace exposes young hackers to the risk of experimenting with cybercriminal activity as simple instructions and tools are readily available on the internet. This 'Crime-as-a-Service' model gives those who are not technically proficient or likely to be involved in traditional crimes access to the tools necessary to commit cybercrime (Europol, 2014).

Developmental psychology often describes the formative teenage years as a time of impulsivity and risk-taking. Therefore, it is important to educate children and young people on the dangers of such activities, as research suggests that many do it for a sense of fun without realising the consequences of their actions or the severe custodial sentences that can result.

10.2 Prevalence

There is evidence to suggest that a growing number of teenagers and young people (particularly boys) are engaging in cybercrime worldwide. For instance:

- In 2015, the Australian Bureau of Crime Statistics and Research reported that cyberfraud offences committed by people under 18 had risen by 26% in the previous two years, and 84% in the previous three years (Harris, 2015).

This is a relatively new phenomenon and as such, there are few academic studies or UK crime statistics on prevalence rates. However, it is worth noting that:

- The National Cyber Crime Unit (NCCU, 2017) stated that the average age of suspects arrested in cybercrime investigations is 17, and there have been several recent cases in which the perpetrators were children.[32]

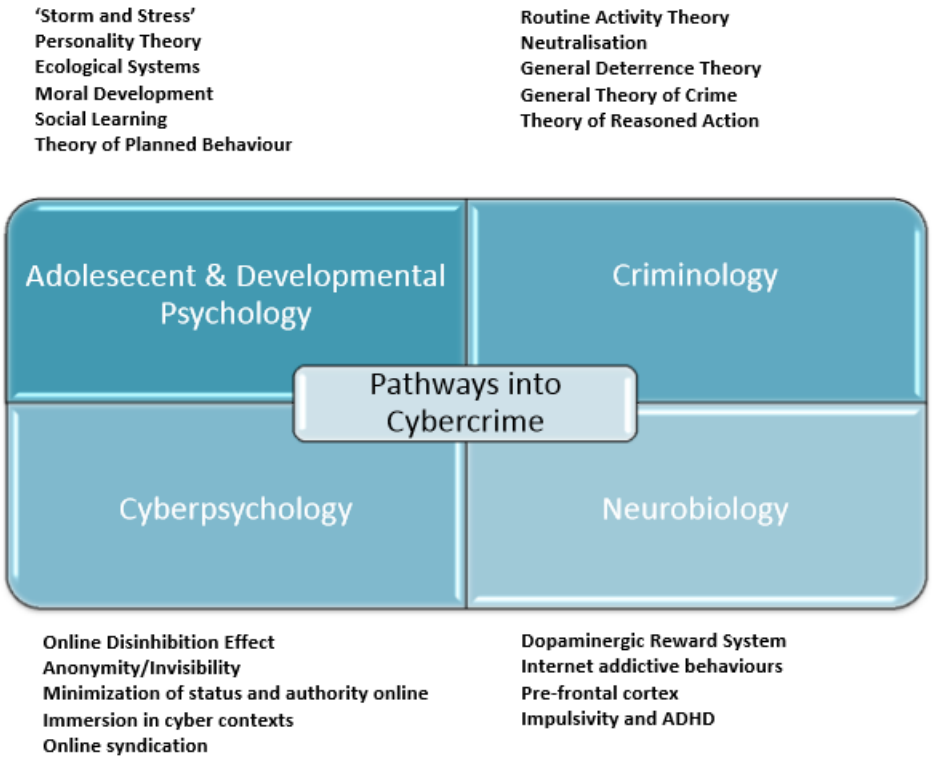
10.3 Key characteristics, behaviours and motivations

To date, most research in the area of cybercriminality among children and young people has relied heavily on qualitative data. A 2016 research project conducted in the UK and Republic of Ireland entitled 'Youth pathways into cybercrime' was established to draw together existing recent evidence on online behaviour and associations with criminal and antisocial behaviour among young people (Aiken, Davidson, & Amann, 2016). This project was undertaken in response to the urgent need to understand the pathways that lead some young people into cybercrime, and to develop effective prevention and intervention strategies.

As seen in Figure 21, the report considered four critical areas of understanding: criminology, developmental psychology, neurobiology, and the emerging realm of cyberpsychology, highlighting that these overlapping areas may be useful to law enforcement and industry in children and young people's hacking prevention processes.

[32] In 2016 TalkTalk was subjected to a cyber-attack perpetrated by two boys aged 16 and 18.

Figure 21: Pathways to cybercrime



Source: Aiken, Davidson and Amann (2016)

Having considered children and young people's hacking in terms of the above paradigm and gathered information from semi-structured interviews with a range of stakeholders, several key findings on the characteristics of young hackers emerged.

Individual characteristics

Hackers tended to:

- be predominantly adolescents
- have high IQ
- be computer literate and curious about technology
- come from a broad range of social classes
- be usually male, socially isolated or awkward, but networked with groups of other like-minded adolescents
- show evidence of some vulnerability
- have a high need for online affirmation and affiliation.

A report by information security company CREST (2015) in conjunction with the National Cyber Crime Unit (NCCU) published findings from a workshop that brought together online security specialists to improve the knowledge base on the motives behind young people's engagement in cybercrime. These are similar to the findings from the 'Youth pathways into cybercrime' study mentioned above. Key common pathways factors identified by stakeholders are listed below.

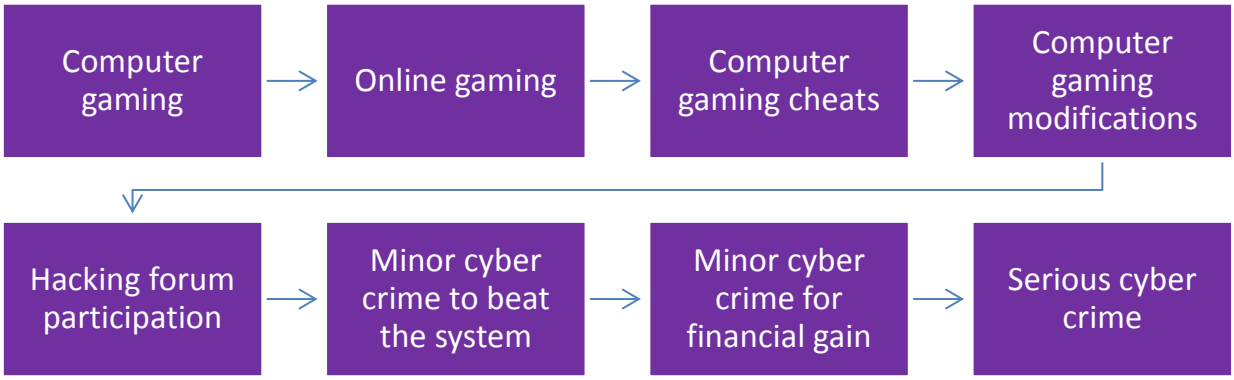
Common pathway factors

- Willingness to engage in low-level illegal internet-related activity that often escalates through *positive reinforcement* by an online peer network.
- Derive intrinsic pleasure from increased *challenge* associated with higher-level online criminality.
- Importance of *online reputation* with peer network compensates for lack of self-esteem in real world and gives a *sense of belonging*.
- Online deviance such as digital piracy is often *minimised*, since the internet is perceived as a place with no guardians or laws.
- Behaviour may become *addictive*.
- Financial gain may not be the goal; rather, the *power* gained by moving up through a hacking network hierarchy is its own reward.

10.4 Gaming as a pathway to illegal activity

The NCCU discovered that a large proportion of the young people identified as being on the periphery of illegal online activity were gaming enthusiasts. This interest in gaming was identified as a significant motive for becoming more interested in computing technology (NCCU, 2017). An example of a possible pathway from gamer to cybercriminal is illustrated below.

Figure 22: Pathways to illegal online activity



Source: CREST (2015)

The National Crime Agency (NCA) suggest that as gamers join hacking forums to source game modifications, they can then be 'groomed' by cybercriminals who recognise their skills and attempt to exploit them by encouraging them to participate in illegal online activities.

10.5 Prevention and intervention

The NCCU has set up a number of interventions to prevent adolescents succumbing to cybercriminality. Young people who have registered information on known illegal websites have had notifications sent to them informing them that the NCA are aware of their activities. In more extreme cases the NCCU engage in 'cease and desist' visits that involve interviewing young people in their homes and if necessary, arrests are made. According to the NCCU, over 80 cease and desist visits have been conducted since 2013 (NCCU, 2017).

As noted by Xu, Hu and Zhang (2013, p. 64), 'Computer hackers start out not as delinquents or as social outcasts but often as talented students, curious, exploratory, respected, and, most important, fascinated by computers.' Therefore, a recurring theme in the limited research available

is that there is a growing and urgent need to promote positive and legal alternatives for channelling young talent toward legitimate careers in the tech sector before they are lured into the area of cybercriminality.

10.6 Summary

Children's involvement in hacking and cybercrime can be summarised as follows:

- Research suggests that many children engage in hacking activities for fun without realising the criminal consequences of their actions.
- Evidence suggests that a growing number of young people are engaging in cybercrime.
- The peer group nature of hacker networks offers excluded young people a sense of belonging and support that further encourages these activities.
- Online games offer a pathway to cybercrime and illegal activities as gaming enthusiasts join hacker forums to source game modifications.
- There is a need to channel the talents of these technologically advanced children into legal and legitimate careers in the tech sector.
- Researchers recommend that metrics should be developed to identify technology-talented young people in the same way that an IQ test measures intelligence.
- Further research is urgently required to explore youth cognitive processes and motivation to engage in hacking. Many traditional criminal theories may need to be reassessed in terms of validation in a cyber context.

11. Vulnerability, victimhood and resilience

11.1 Who is vulnerable online?

Some children appear to be specifically 'at risk' online, being either more likely to encounter risk or when they do encounter risk, more likely to find it harmful. In short, they may be less resilient or less able to cope. Those who encounter risks offline are likely to encounter them online, and those who encounter one risk online are also likely to encounter other risks (Livingstone & Palmer, 2012; Livingstone & Smith, 2014).

We examine what is now known about the ways in which some children may be particularly vulnerable, off and online. In the 2012 UKCCIS review, we noted that Palmer, Piggin and Hilton (as cited in Livingstone & Palmer, 2012) identified four broad groups likely to be less resilient to risks online (and offline). These remain the most likely sources of vulnerability, although it is still true that little research has examined their online experiences in much detail:

- *Children who experience family difficulties* or who are brought up in chaotic family/home environments may suffer physical, emotional and/or sexual abuse and neglect, witness domestic violence and/or family breakdown, be brought up in an environment in which drugs and alcohol abuse of the adults around them impinges on the quality of parenting they receive and may be children who, having been judged to have suffered significant harm, are placed in the care system.
- *Children with disabilities* – they may suffer from chronic physical ill health, have physical or learning disabilities or special educational needs.
- *Children with emotional/behavioural difficulties* – these children may present with differing symptoms such as a propensity to self-harm, to be prone to suicide attempts, to have a diagnosed mental or behavioural condition.
- *Children who experience exclusion of access* – these children experience system neglect in the sense that they are unable to access services that are universally available to other children. They belong to the more marginalised groups within society such as travellers, asylum-seekers, trafficked or migrant communities.

We note a small study conducted by the Lucy Faithfull Foundation with young people aged 13-16 with SEN that points to specific difficulties with social interaction, namely, that these children:[33]

- may believe everything that they are told and take conversations at face value
- tend to have poor social skills and interpretations of inappropriateness can be worse online when there are fewer boundaries or visual cues, and not so immediate consequences or repercussions
- are often desperate for friendship, which can make them vulnerable to accepting friends on Facebook and other SNSs, as this can make it appear that they are popular
- may be unable to detect appropriate behaviour from other internet users
- tend to regard games as more real than their mainstream peers; they struggle to see things as fantasy and lack the ability to be imaginative
- can become obsessed with the internet or with particular people they meet, and may be considered to be stalking someone
- are often obsessive and compulsive, and may be viewed as addicted
- have an absence of supportive adults in their lives.

[33] A focus group was held with seven girls and three focus groups were conducted with teachers at three schools for children and young people with SEN. See Research Highlight #20.

Research by Quayle, Jonsson and Lööf (2012) with young victims of online grooming supports this work and describes the way in which young people can become drawn into abusive relationships, often feeling trapped, 'caught in a web' and unable to confide in family and friends. This research also suggests that vulnerable young people are more likely to respond initially feeling that there is a 'gap' in their lives. This finding is consistent with findings from Webster et al.'s (2012) research with convicted groomers that suggested that offenders deliberately target young people perceived to be vulnerable.

More recent research conducted by Whittle, Hamilton-Giachritsis and Beech (2014) conducted with child victims of online groomers suggests that the reasons why participants engaged with offenders varied and included loss of family protection (whether due to relationship instability or monitoring habits of parents), and online risk-taking behaviour was found to be central in contributing to vulnerability. Based on a small number of six qualitative interviews, three victim vulnerability scenarios were identified: (1) multiple long-term risk factors; (2) trigger events; and (3) online behavioural risks. They argue that young people across vulnerability scenarios can be better protected through consistent, collaborative approaches by parents, carers and other adults in their lives.

11.2 Typologies

Recent EU-funded research conducted on a larger scale has identified new typologies of cybervictimisation that considers the influence of multiple factors from both the real and virtual lives of young people, these findings are based on surveys with young people conducted in three EU countries. The following broad groups were identified:

- The *adapted adolescent* group was the largest and had the least number of risk behaviours online or offline, were the least vulnerable and least likely to receive sexual solicitations from an adult online.
- The *inquisitive non-sexual* group had lower risk taking offline but higher online risk taking. They were at low likelihood of receiving sexual solicitations or sending sexts.
- The *inquisitive sexual* group demonstrated the highest rate of receiving requests for sexual information. They had a high likelihood of receiving sexual solicitations from adults. It is concerning that this group also had the highest likelihood of meeting up in person to engage in sexual activity.
- The *risk-taking aggressive* group was the smallest. They exhibited the highest risk taking on- and offline, and were most likely to both harass and be harassed. They demonstrated real-world antisocial behaviour such as problems with authority (parents and teachers), truancy, school exclusion, drug and alcohol misuse. They had the highest levels of online/offline aggression towards others, including peers. They also had a heightened level of experiencing online/offline victimisation at the hands of others.

11.3 Online vs. offline vulnerability

There is limited research in the UK exploring which children appear to be more vulnerable online, and seeking to understand their experience, this research is essential if practice and policy is to respond appropriately. As Carrick-Davies' (2011) small-scale mixed methods project further suggested, those vulnerable offline are also likely to be vulnerable online due to several factors:

- absence of supportive adults in their lives
- more unsupervised time and less regular routines or directed activities
- staggered entry to learning environments, potentially missing out on e-safety advice
- tendency to crave group identity and to be viewed as outsiders or risk takers

- likely to experience abusive environments including being on the receiving end of violence
- greater exposure to influences of alcohol, drugs, early sexual experience and gang culture.

Research conducted by Palmer (2015) suggests that three other groups of young people are vulnerable online, including those who are diagnosed as being on the autistic spectrum; those young people with mental health issues who rely on the internet for fulfilling aspects of their lives they do not feel able to meet offline; and those young people exploring their sexual orientation.

11.4 Self-harm

When evaluating the risks to children online, it is also important to take into account the issue of self-harm, suicides and eating disorders, among others. According to a survey conducted by Livingstone et al. (2011) for EU Kids Online, 7% of the children surveyed have seen sites relating to self-harm while 5% have seen sites relating to suicides. According to Mascheroni and Ólafsson (2014), seeing potentially negative user-generated content (related to hate, pro-anorexia, self-harm, drug-taking or suicide) is the third most common risk reported by children aged 11-16. In the UK, as noted earlier, 11- to 16-year-olds' exposure to such content has risen slightly between these two studies. Some of the primary causes of suicidal ideation are:

- cyberbullying
- grooming and online abuse
- emotional and behavioural difficulties.

In a study conducted by Biddle et al. (2012), 13 of the 22 individuals interviewed who had survived 'near fatal' suicide attempts reported using the internet as a source of information. There is also increased evidence that the individuals using novel suicide methods have researched them on the internet (Chen et al., 2013; Gunnell et al., 2014).

Although technical controls exist for blocking such content through home network-level filters, support systems are required to help a child recover. A summary of the practice findings of the UKCCIS Evidence Group seminar (Livingstone & Palmer, 2012) noted that health/nursing staff failed to recognise the importance when their suicidal patients disclosed their online activities.

Although helpline-related support services have already made a positive impact in this area (see Dinh et al., 2016), an enabling environment from parents and carers would prove to be especially beneficial for vulnerable children. However, although online communities dedicated to suicide, self-harm and eating disorders such as bulimia/anorexia can be seen to perpetuate harmful behaviour, they also act as support systems for excluded and marginalised children by providing them with peer support and positive identity formation (Bond, 2012; Polak, 2007). In a systematic review conducted by Daine et al. (2013) on the influence of the internet on self-harm and suicide in young people, it was found that methodologies used by studies in this area affect the inferences drawn. In their review Daine et al. found purely quantitative studies are more likely to find a negative influence compared to a qualitative or mixed methods study.

Thus, it is important to understand children's motivations behind the use of and access to self-harm information online and their membership of communities centred round such practices. The lesson these online communities provides for safeguarding approaches suggest a model that can be adapted for providing peer-to-peer online support systems for children.

11.5 Digital resilience

It is clear that a minority of children and young people are more vulnerable to online abuse than other children. Early research in this area suggests that those young people who are vulnerable in

the real world are also vulnerable online. Research using the survey approach demonstrates that the majority of young people have some digital resilience in negotiating online risk environments.[34]

The 3rd Youth Internet Safety Survey (Priebe, Mitchell, & Finkelhor, 2013) in the US investigated responses to reported unwanted internet experiences:

- The most often mentioned response to sexual solicitation was active coping, mainly blocking or warning the person/telling the person to stop (42%); 29% of those who had experienced online harassment used active coping, while 38% used other unspecified responses.
- Incident characteristics and most children and young people's characteristics were not related to whether they used active or passive coping.
- Distressed children and young people more often used active coping if they could not stop thinking about the incident (e.g., 28% who experienced sexual solicitation, 37% who experienced online harassment), did not want to use the internet because of the incident (36% who experienced sexual solicitation), or felt jumpy/irritable/had trouble sleeping (35% who experienced online harassment).
- Passive coping (e.g., leaving the site, logging off) was the response most often used in response to unwanted exposure to pornography (77%).

In a study by d'Haenens, Vandoninck and Donoso (2013), it was noted that vulnerable children were more likely to use passive coping strategies than children with higher self-efficacy who were more likely to use active coping strategies. It was also noted that children with parents who sporadically used the internet were more likely to be employing passive coping strategies.

While is it clear that the majority of young people appear to be resilient to online approaches and harassment, there is limited research but an emerging engagement with the issue (see, for example, Children's Commissioner, 2017 and Day, 2016 for the UK and d'Haenens, Vandoninck, & Donoso, 2013 for the EU) that focuses on the need to create enabling environments for vulnerable children, and support strategies that increase children's self-efficacy in dealing with online risks that are associated with children's online experiences that are part of their daily lives. However, most large-scale projects in this area have been undertaken in the EU (funded by the EC) and US.

11.6 Summary

Finding on children's vulnerability, victimhood and resilience are as follows:

- Children belonging to identified vulnerable groups are likely to be less resilient to online and offline risks.
- Those who encounter risks offline are likely to encounter them online, and those who encounter one risk online are also likely to encounter other risks.
- Groomers deliberately target young people perceived to be vulnerable.
- It was found that those vulnerable offline are also likely to be vulnerable online.
- Vulnerable children are more likely to use passive coping strategies in response to online risks.
- There is evidence that children gain digital skills and coping strategies as they grow older, adding to their digital resilience. There is little evidence, however, that children's digital skills and resilience are improving over time.

[34] For example, Livingstone et al. (2010, 2012b, 2014b, 2017); Livingstone and Palmer (2012); Day, 2016, among others.

12. Initiatives to safeguard children online

Sustained efforts are required from all stakeholders involved in order to effectively safeguard children online in a dynamic technological landscape and the ever evolving risks associated with it. There is a growing body of evidence regarding the nature and evaluation of initiatives designed to safeguard children on the internet. The policy and practice of online child safety has seen dynamic engagement from concerned policy-makers, parents, educators, experts and law enforcement officials. Thus, it is important to evaluate initiatives and to understand the reasons for their success or failure. However, in relation to children's internet safety, rather few initiatives have been independently evaluated, making it difficult to set out a firm basis for future actions.

12.1 Trends in children's digital literacy

Digital literacy can be understood as the ability of individuals to use skills, knowledge and understanding in order to make full use of the opportunities offered by the new media environment as well as safeguard themselves from associated risks (see Buckingham, 2007; Buckingham et al., 2004). In the UK there has been a patchy history of digital literacy and media education initiatives (McDougall et al., 2014) and recent calls to put digital media education firmly on the curriculum (Children's Commissioner, 2017; House of Lords, 2017).

Children's skills vary according to their gender, age and SES:

- Girls tend to report slightly fewer digital skills than boys, and younger children report considerably fewer than older teenagers.
- Skills of children with disabilities, who are discriminated against, or who are from disadvantaged backgrounds, vary – some have fewer skills commensurate with their fewer resources or available supports, but others have developed skills partly through facing negative experiences online (Livingstone, Görzig, & Ólafsson, 2011).

Focusing on the use of SNSs, Livingstone (2014) shows that children's digital literacy changes qualitatively with age:

- at around 9-10, children are concerned with what's real or not, although they may not discriminate real from fake clearly
- at 11-13 they are more concerned with what is fun or even transgressive, irrespective of whether it is trustworthy
- by 14-16 their increasing maturity leads teenagers to refocus on what is more valuable for them or more generally.

This shift in focus is brought about by a change in peer and parental relations, and has implications for the incidence of online risks encountered by children. Ofcom's surveys over recent years have sought to track changes in children's media literacy on a range of indicators (see Ofcom, 2016a). The findings suggest that:

- Children's digital literacy increases fairly steadily from age 8 to young adulthood. For example, they become gradually less likely to think that all information on news media sites is true and more likely to know that sponsored results on Google are adverts that have paid to be there.
- Relatedly, with increasing age, children gain the digital literacy to realise that some but not all search engine results can be trusted. However, there is no strong increase in understanding through the early teens, the main gain being among younger children.

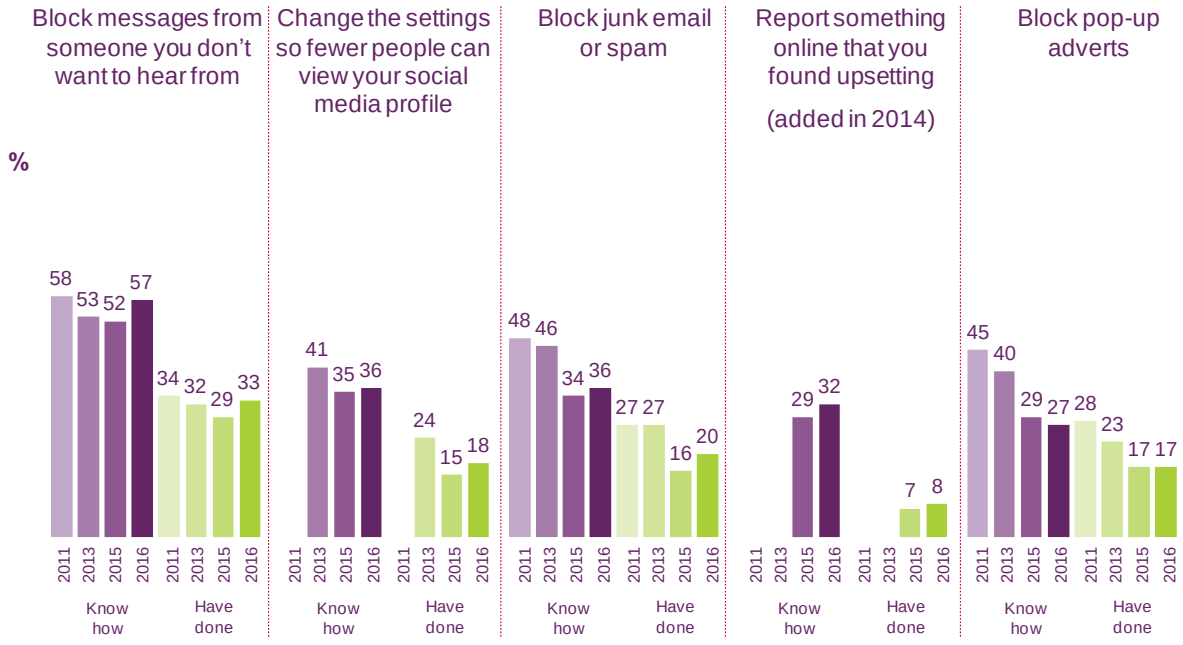
- Through questions asked only of 12- to 15-year-olds, the Ofcom data suggests that children are more likely to recognise by age 15 that advertising is personally targeted and that vloggers are paid to promote products.
- However, from 12-15 children become more likely to value getting 'likes' online and more likely to provide personal data in order to gain 'followers'.

Thus, while children come to understand the digital environment better with age and experience, it is by no means clear that a critical understanding of the digital environment results in cautious behaviour regarding personal data protection. Indeed, the data show how uneven children's digital literacy is. For instance, while more than three quarter of 12- to 15-year-olds are cautious about their privacy and data sharing when visiting new websites, the majority (58%) believe information online can be easily removed if they no longer wish to share it with other people.

In short, children usually tend to apply critical thinking depending on context or mood. While they learn more as they grow older, they may also experience a strong desire to fit in, limiting their willingness to stop and think critically.

Gaps between children's ability, knowledge and skills are also evident in relation to online safety. Ninety-four per cent of 8- to 15-year-olds have received information on how to stay safe online, with parents and teachers being the primary source of information and social media being the last (Ofcom, 2016a). However, as Figure 23 shows, while up to half of 12- to 15-year-olds are aware of the technical means to protect themselves online, fewer have actually done this.

Figure 23: Experiences of 'safe' online measures among children aged 12-15, 2011, 2013, 2015 and 2016

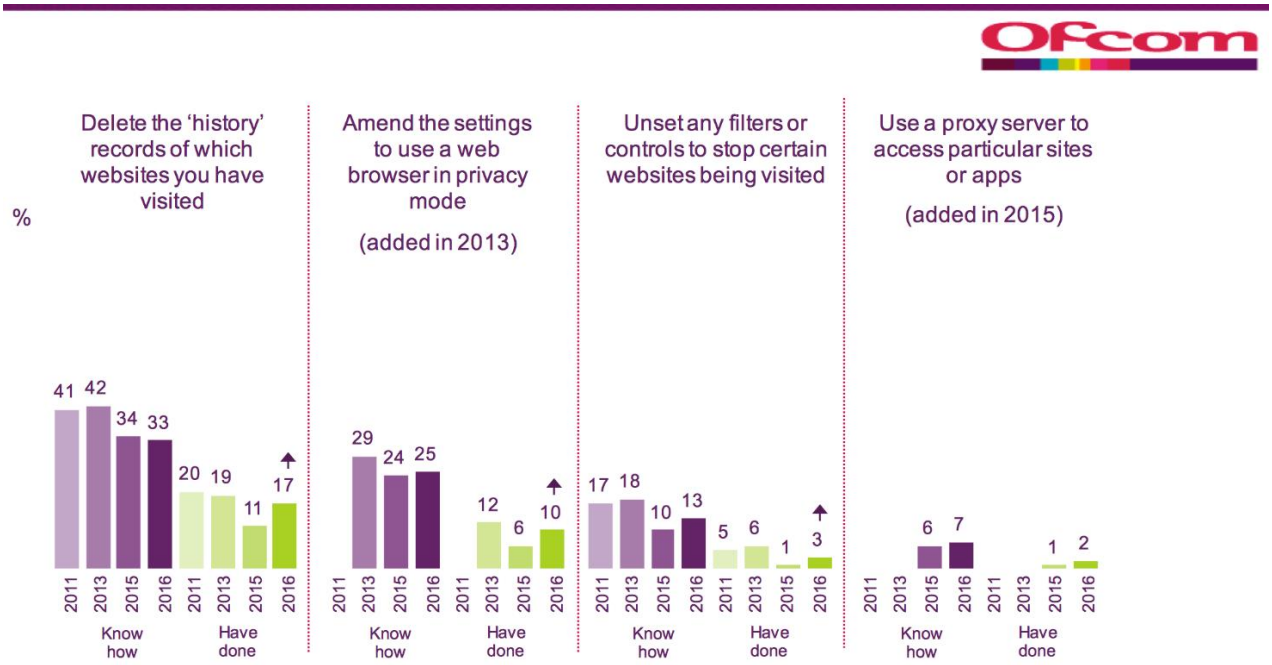


QC61/62: Please take a look at the list of things shown on this card and think about whether you know how to do any of these things online. Please read out the numbers on the card if you know how to do this. And are there any things on this list that you personally have done online in the last year? Please read out the numbers on the card if you have done this in the last year (prompted responses, multi-coded).
Base: Children aged 12-15 who use the internet at home or elsewhere (463 aged 12-15 in 2016). Significance testing shows any difference between 2015 and 2016.
Source: Ofcom (2016a)

Figure 23 also offers little evidence of improvement in children's digital skills in the past five years. This applies to children's supposed abilities to 'get around' technical controls designed to protect

them, as shown in Figure 24. This shows that children's ability to evade technical controls is fairly low.

Figure 24: Experiences of 'risky' online measures among children aged 12-15, 2011, 2013, 2015, 2016



QC61/62: Please take a look at the list of things shown on this card and think about whether you know how to do any of these things online. Please read out the numbers on the card if you know how to do this. And are there any things on this list that you personally have done online in the last year? Please read out the numbers on the card if you have done this in the last year (prompted responses, multi-coded).
Base: Children aged 12-15 who use the internet at home or elsewhere (463 aged 12-15 in 2016). Significance testing shows any difference between 2015 and 2016.
Source: Ofcom (2016a)

Findings comparing EU Kids Online and Net Children Go Mobile also show little change in the levels of children's digital literacy and safety skills since 2010, although children are now better able to manage their privacy settings and to delete their browsing history. On the other hand, the same comparison shows that the proportion of children whose profiles are public has nearly doubled from 11 to 19% of social network users aged between 9-16, which may reflect the diversification in social networks used (Livingstone et al., 2014c).

There is still a need to foster safe online practices and to support children's constructive responses to risks they encounter online:

- a relatively small percentage of children (13%) who have encountered online risk have reported it
- the majority of children who are SNS users (42%) have a public profile as opposed to 32% who have private profile and 26% who do not understand the difference
- of those children who encountered sexual imagery online, most hoped it would go away (26%), with half the number actually reporting the incident (13%). Others tried to fix it (22%), deleted unwelcome messages (19%) or blocked the sender (15%)
- it was noted that higher skills were correlated with higher risks being encountered online (Livingstone et al., 2012b).

In other research, 10- to 13-year-olds represented a higher risk group than 14- to 16-year-olds because they are more likely to add unknown people as friends and share their personal information more freely (Martellozzo, 2012).

A study conducted in the US throws some light on the gap between children's risk recognition and actual practices. Although children are aware of and concerned about online risk (67% are concerned about their privacy, 59% about strangers learning something about them, and 53% about harmful content), 49% of the teens (aged 13-17) surveyed reported befriending a stranger online, 43% reported posting something online that they later regretted, 25% shared their personal details such as school and 21% shared personal details such as a phone number online (FOSI, 2012).

12.2 Educational initiatives for children

Schools are an important partner in ensuring child protection online (see DfE, 2014; Shipton, 2011). E-safety guidance from schools is particularly helpful for children from under-resourced households where parents lack confidence or expertise with relation to digital media (Livingstone et al., 2015; see also Opinion Leader, 2013). Whittle, Hamilton-Giachritsis and Beech (2014) found that support from schools along with support from parents and friends also assisted with the recovery of victims of online grooming and sexual abuse.

According to the Byron Review (2008), in order to raise the skills and capabilities of parents and children the government should focus on:

> … delivering e-safety through the curriculum, providing teachers and the wider children's workforce with the skills and knowledge they need, reaching children and families through Extended Schools and taking steps to ensure that Ofsted holds the system to account on the quality of delivery in this area. (2008, p. 8)

Schools use a range of e-safety strategies and initiatives (Ofcom, 2014a, pp. 56-7), such as:

- annual talks, some with members of the police and/or NSPCC representatives
- information videos and associated lesson plans:

  > "We saw a video on CBBC about a girl and 1Direction and she gave out her details and didn't realise." (Girl, 8-9 years old, Nottingham)

- e-safety pupil representatives:

  > "I am e-Safety rep at school and we help to tell [others] how to be safe online." (Girl, 8-9 years old, Nottingham)

- take-home 'contracts' to share with parents to agree terms of safe internet use (see also Shipton, 2011).
- a Safer Internet Day, held once a year, and other campaigns.

A small-scale qualitative study involving two primary school by Shipton (2011) highlighted the e-safety best practices schools can adopt in order to effectively protect children online:

- It was found that the schools preferred developing the critical capabilities of the students rather than employing blanket filters. This was done to ensure that children are able to manage risks both at school and elsewhere.

- One of the schools reported using a Managed Learning Environment (MLE) around e-safety that encouraged students to report incidents that made them unhappy or uncertain online.
- Both schools used a video by CEOP to address issues around internet safety for teachers and primary school children.

However, although it was found that schools used common sense when approaching e-safety, it was recommended that they have dedicated e-safety policies so that any problems could be addressed quickly. It was also recommended that schools update their Acceptable Use Policies once a year in order to integrate any digital concerns that may arise (see also DfE, 2014). It was advised that schools include Staff User Agreements outlining best practices for teachers.

A National Foundation for Educational Research (NFER) survey of 1,315 teachers from 1,051 mainstream schools by Aston and Brzyska (2012) further strengthens the argument for developing critical capacities among children:

- The vast majority of teachers felt that their pupils had the skills and knowledge to use the internet safely in school, but only 58% felt that the children were similarly equipped to use it safely at home.
- The survey also noted that the likelihood of secondary schools having e-safety policies was lower than primary schools.
- This trend is reflected in teacher's e-safety training – 77% of primary school teachers and 54% of secondary school teachers felt that the staff had received adequate e-safety training.
- Although teachers felt confident in advising students on e-safety, this did not extend to the safe use of SNSs.

The last two findings are especially worrying because 91% of secondary school teachers and 52% of primary school teachers report that pupils at their school have experienced cyberbullying, with SNSs being the most common platform.

The cyber survey for Suffolk found that although 92% of pupils report receiving e-safety education in school, parents of 40% of 10- to 11-year-olds do not address the issue of e-safety at home (Katz, 2014). Thus, while parents are often the primary source of information about online risks, schools are the primary source of information for e-safety.

Campaigns such as the Safer Internet Day help in bringing about a change in online practices. Of those who were aware of the Safer Internet Day (UK Safer Internet Centre, 2016b):

- 87% of 8- to 17-year-olds said they were more confident about what to do when they were concerned about something online
- 83% said that they were more confident about how to stay safe online
- 41% of 8- to 17-year-olds changed something about the way they used the internet after hearing about Safer Internet Day.

In general, schools should aim to provide broad e-safety advice (e.g., about commercial risks, about how online conflicts between peers can escalate) and offer forms of support. Through e-safety, schools should highlight the good points about the internet and avoid creating a moral panic by overstressing the online world as a dangerous and misleading place (Smahel & Wright, 2014). Given the rising incidence of cyberbullying and online risk, 'cyberbullying should now form part of all PSHE curriculum with regularly updated content to reflect the constant changing nature of social media' (Ditch the Label, 2013, p. 14).

12.3 Trends in parental mediation of children's activities

Due to the opportunities and risks associated with children's digital media use, parenting strategies require a constant balancing act between protecting children from online harms while at the same time not restricting the educational, social and creative opportunities they stand to gain from using digital media (Livingstone & Helsper, 2008). Parents use a combination of approaches to mediate their children's online access and use of digital media (Ofcom, 2016a). This includes both restrictive and enabling mediation strategies (Livingstone et al., 2017), and falls under four categories (Ofcom, 2016a, p. 174):

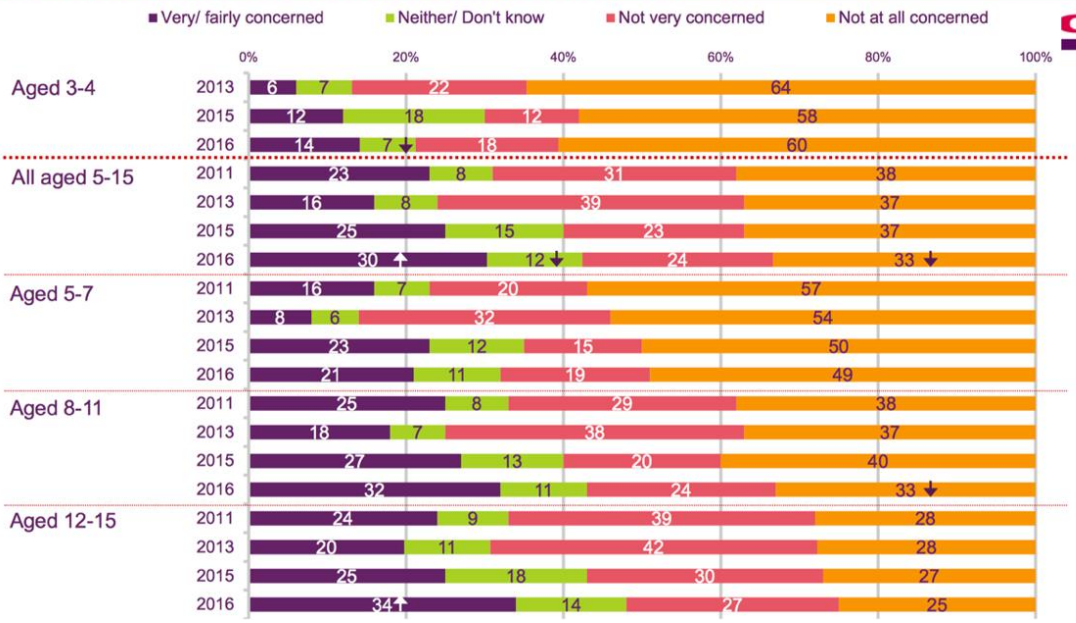
- technical tools including content filters, PIN/passwords, safe search and other forms of technical mediation
- regularly talking to the child about managing online risks
- rules or restrictions around online access and use
- supervision when online.

Restrictive mediation strategies refer to a range of online activities that parents may restrict or ban while enabling mediation strategies involve actively talking to the child about what they do online, encouraging safe practices and giving safety advice (Livingstone et al., 2017). Enabling strategies can also include technical controls that are aimed towards building a safety framework so that positive uses of the internet can be encouraged.

Significant gaps exist in parental risk perception and parental mediation strategies, however:

- According to Figure 25, only 14% and 18% of parents of 3- to 4-year-olds and 30% and 24% of 5- to 15-year-olds are very concerned/fairly concerned and not very concerned about content respectively.
- This indicates that a significant proportion of parents are not at all concerned about online content, although this proportion appears to decrease with age (60% not concerned for 3-4 year olds and 33% for 5- to 15-year-olds).
- Encouragingly, 99% of parents of 3- to 4-year-olds and 96% of parents of 5- to 15-year-olds actively implement at least one form of mediation strategy (Ofcom, 2016a).

Figure 25: Parental concerns about online content among those whose child goes online at home (2011, 2013) at home or elsewhere (2015, 2016), by age



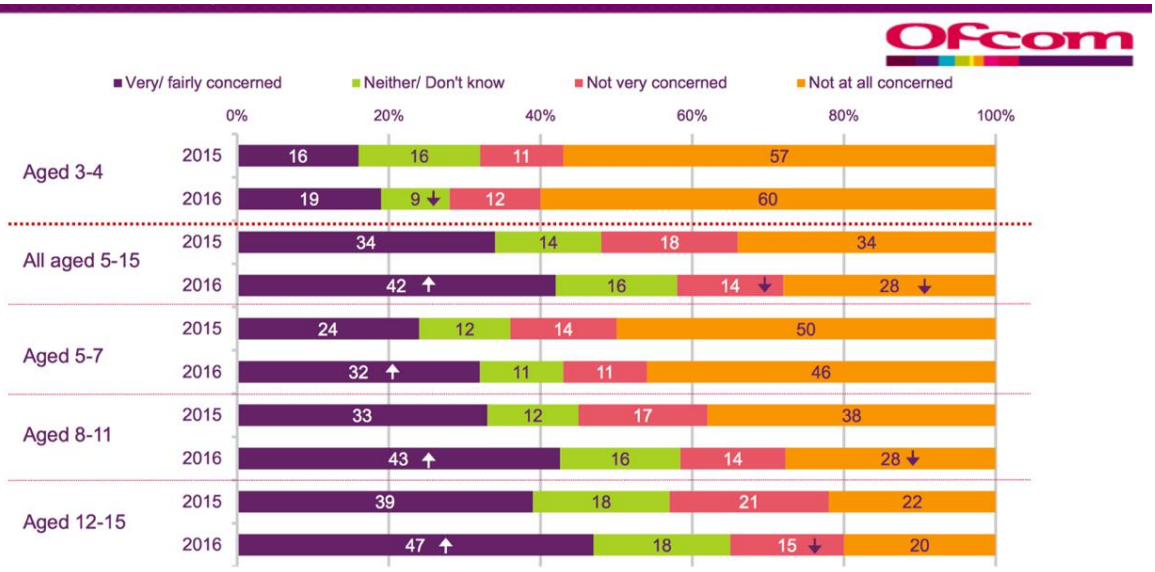
QP51A: Please tell me the extent to which you are concerned about these possible aspects of your child's online activities – The content on the websites or apps* that they visit (prompted responses, single-coded). * Apps was added in 2015.

Base: Parents of children who go online (272 aged 3-4, 1,168 aged 5-15, 264 aged 5-7, 444 aged 8-11, 460 aged 12-15 in 2016). Significance testing shows any difference between 2015 and 2016.

Source: Ofcom (2016a)

A similar observation applies in relation to parental concerns about companies collecting their children's personal information (see Figure 26).

Figure 26: Parents' concerns about companies collecting information about what their child is doing online, by age, 2015 and 2016



QP51I: Please tell me the extent to which you are concerned about these possible aspects of your child's online activities – Companies collecting information about what they are doing online (e.g., what they have been looking at online/sites they have visited etc.).
Base: Parents of children who go online (272 aged 3-4, 1,168 aged 5-15, 264 aged 5-7, 444 aged 8-11, 460 aged 12-15 in 2016). Significance testing shows any difference between 2015 and 2016.
Source: Ofcom (2016a)

Parents' knowledge and use of technical controls tend to differ:

- although the majority of parents are aware of parental control software (61% among parents of 3- to 4-year-olds and 59% among parents of 5- to 15-year-olds), they are less likely to use it than home network-level filters.

Parents have an overall positive attitude to network-level filters:

- over 90% of the parents who use technical controls such as parental control software or network-level filters have found them useful
- more than three quarters of the parents of 5- to 15-year-olds who use content filters say it blocks the right amount of content. The majority of the parents who use content filters are confident that their child cannot get around them (see Figure 27).

Parents who do not use content filters report using other mediation strategies:

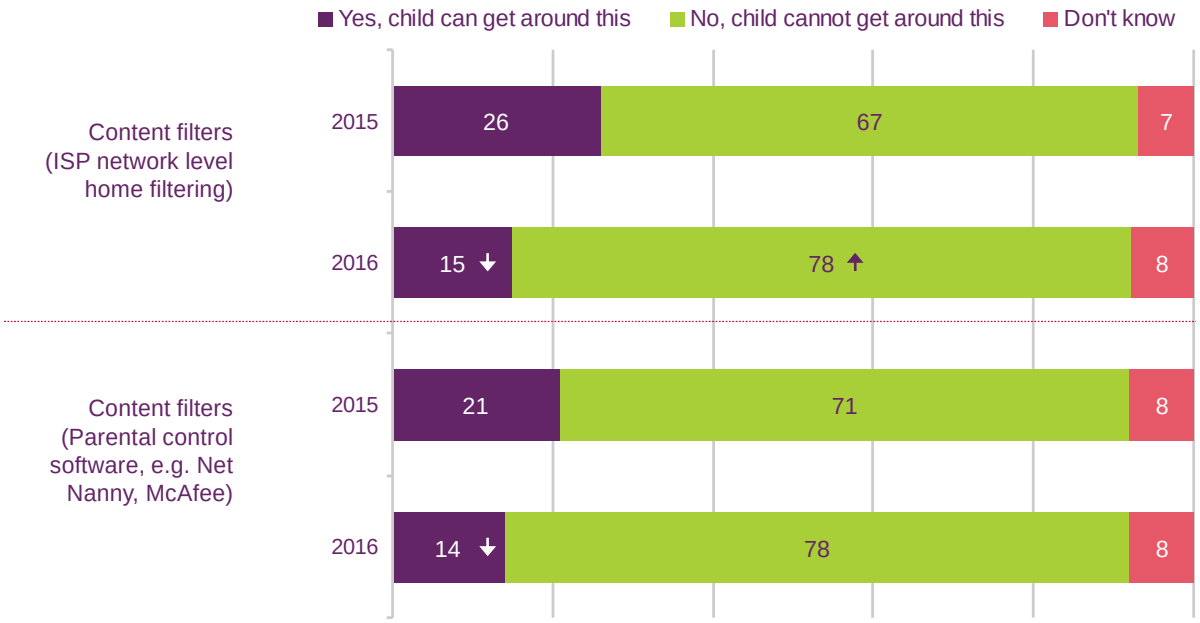
- the majority of such parents (60%) prefer to talk to their children and use supervision and rules
- close to half (48%) trust their child to be responsible
- only 5% feel that they would not work or their children might find a way to get around them
- comparatively larger proportions of parents are not aware of technical controls other than network content filters and parental control software (see Figure 28).

Mediation strategies tend to become ad hoc especially with relation to younger children (under 9), even though internet access is rising among them as result of increased tablet use. A study conducted by Livingstone et al. (2014d), focusing on families with children under eight, found that:

- many parents believed that robust strategies need not be developed until the child is older
- violence and strong language were of greater concern to parents of young children than sexual content and unwanted contact.

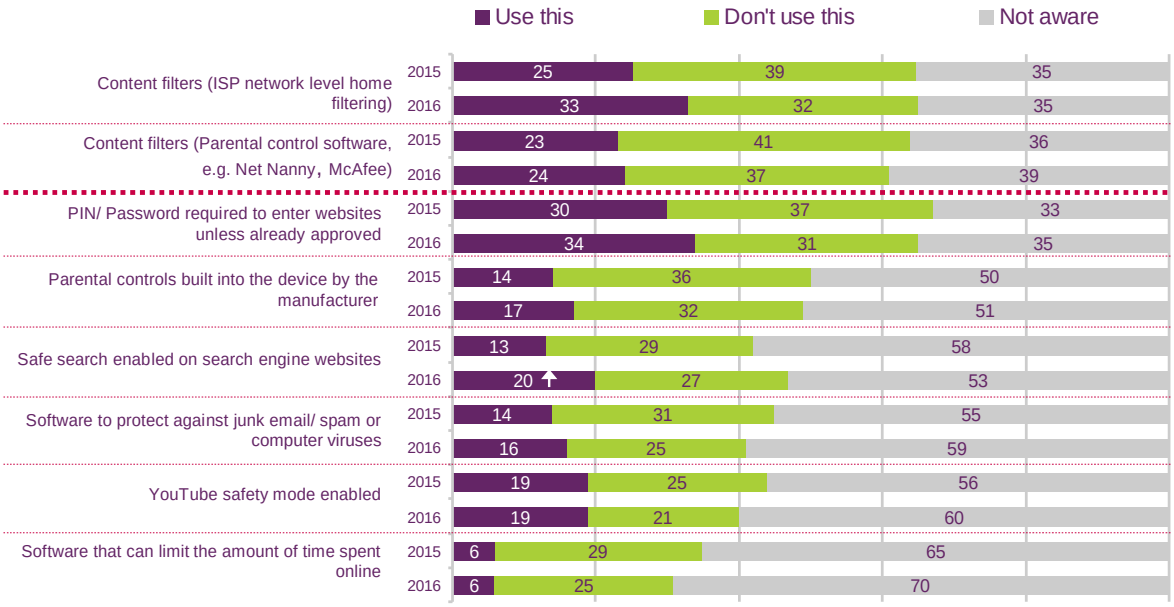
The development and promotion of education materials for parents and carers, which include safety settings, passwords, privacy protection and content, would surely be helpful.

Figure 27: Parents of 5- to 15-year-olds who use content filters – perceptions of child's ability to bypass technical tools, 2015 and 2016



QP36A-B: Do you think your child can get around them? (unprompted responses, single-coded)
Base: Parents of children aged 5-15 with a broadband connection at home and who use each technical tool or control (variable base). Significance testing shows any change between 2015 and 2016.
Source: Ofcom (2016a)

Figure 28: Parents of 3- to 4-year-olds who have home broadband and whose child goes online – use and awareness of technical controls, 2015 and 2016



QP31A-H: Please read each of the descriptions shown on this card. Before today were you aware of any of these types of technical tools or controls? Which ones? (prompted responses, multi-coded)
QP32A-H: Do you use any of these types of technical tools or controls to manage your child's access to online content? Which ones? (prompted responses, multi-coded)
Base: Parents of 3- to 4-year-olds with a fixed broadband connection available to their child at home that the child uses to go online (248). Significance testing shows any change between 2015 and 2016.
Source: Ofcom (2016a)

Smartphones and tablets present their unique risk environments as most network-level filters do not apply to applications used on such devices. Apart from the technical controls discussed above, three controls specific to app management are as follows:

- changing the settings on a phone or tablet to stop apps being downloaded
- changing the settings on a phone or tablet to prevent in-app purchases
- parental control software to restrict app installation or use (Ofcom, 2016a, p. 186).

Nearly 60% of parents are not aware of these tools, and less than 17% actively use them. Nearly half the parents (52%) of 5- to 15-year-olds were aware of an adult content control bar on mobile phones. However, only 39% had activated it; 19% said it was deactivated and 42% reported not knowing whether the bar was in place or not.

Apart from technical controls, parents tend to employ enabling strategies (Ofcom, 2016a), and most have discussed online risks with their child (see Table 9):

- Compared to 2015 data, parents are more likely to have spoken to their children about a wider range of risks in 2016, although the percentage of parents having spoken to their children about online risks remains close to the 2015 level, at 84%.
- The frequency of parents talking to their children about online risks increases with age, from 14% of parents of 3- to 4-year-olds to 40% of parents of 12- to 15-year-olds.
- Half of the parents who have never spoken to their children say it is because their child is too young for this type of conversation; about a fifth say it is because they are always supervised online.

Table 9: Parents talking to their children about managing online risks, by ages, 2016

All who go online	Aged 3-4	Aged 5-15	Aged 5-7	Aged 8-11	Aged 12-15
Base	272	1168	264	444	460
Content on sites or apps that might be unsuitable for their age	16%	56%	46%	60%	59%
Talking to or meeting people they only know online	8%	56% ↑	27%	60%	68% ↑
Sharing too much information online	7%	55%	26%	56%	69% ↑
Believing everything they see or hear online	10%	54% ↑	38%	52%	63% ↑
Being bullied online/ cyberbullying	6%	52% ↑	27% ↑	52%	66% ↑
The possibility of them bullying others online or making negative comments about other people online	2%	38% ↑	20% ↑	37%	47% ↑
Downloading or getting viruses or downloading other harmful software as a result of what they do online	5%	35% ↑	18%	34%	45% ↑
Sending inappropriate personal pictures to someone they know	3%	32% ↑	12%	30%	46% ↑
How their online use now could impact them in the future	3%	30% ↑	13% ↑	30% ↑	40% ↑
Trying to access inappropriate content/ bypass filters	2%	30% ↑	19% ↑	30%	36% ↑
The pressure to spend money online	4%	27% ↑	14%	27%	34% ↑
Illegal online sharing or accessing of copyrighted material	2%	22% ↑	7%	22% ↑	30% ↑
TOTAL – HAVE TALKED TO CHILD ABOUT ANY OF THESE RISKS	27%	84%	65%	86%	91% ↑

QP28: Have you ever talked to your child about any of the following things that could happen online? (prompted responses, multi-coded)
Base: Parents whose child goes online (272 aged 3-4, 1,168 aged 5-15, 264 aged 5-7, 444 aged 8-11, 460 aged 12-15). Significance testing shows any change between 2015 and 2016.
Source: Ofcom (2016a)

Parental strategies also involve creating rules regulating their children's internet access and use of phones and gaming devices. Rules tend to vary with age:

- 83% of parents of 5- to 15-year-olds compared to 73% of parents of 3- to 4-year-olds have rules about using the internet
- younger children have rules relating to content, contact and online purchasing
- for older children, the rules for online safety become wider, more specific and pronounced
- for the 12-15 cohort, rules rise in tandem with parental concerns, with a higher propensity for rules regarding contact with strangers (51%), online purchasing (50%) and how to behave online (42%).

More than three quarters of parents of 8- to 15-year-olds have rules in place specifically regarding the use of mobile phones. However, most of the rules concern managing costs associated with mobile phones rather than the possibility of encountering violent content online.

Parental control on gaming devices also vary primarily according to the child's age:

- parents have more controls for 3- to 4-year-olds (42%) and least for 12- to 15-year-olds (30%)
- less than a fifth of the parents with children with gaming consoles do not have safety controls. Of those, 42% say it is because they trust their child to be sensible/responsible, and 16% responded that they didn't know this was possible/how to do this

- the incidence for having rules and restrictions for playing games tends to decrease with age in the older cohort (88% for 3- to 4-year-olds vs. 73% for 12- to 15-year-olds).

Another parental mediation strategy involves supervision of children's online use. Eighty-three per cent of parents of 5- to 15-year-olds supervise their online activity:

- 52% reported being nearby to constantly check what they are doing
- 45% reported asking their children what they are/have been doing
- 33% reported checking the browser history
- 26% reported sitting beside them and watching them/helping them while they were online.

12.4 Sources of parental support – actual, desired

Further data from Ofcom (2016a) reveals parents' information-seeking with regard to online safety:

- 72% of parents of 5- to 15-year-olds say that they have looked for or received advice on how to help their children manage online risks compared to 45% of parents of 3- to 4-year-olds
- parents' likelihood of seeking information on online safety increases with age: 75% of parents of 8- to 11-year-olds and 73% of parents of 12- to 15-year-olds say they looked for information or advice from other sources compared to 45% of parents of 3- to 4-year-olds and 64% of parents of 5- to 7-year-olds
- schools were the primary source of information across all age groups.

There are notable gaps between parents' abilities and skills for effective mediation (Ofcom, 2016a):

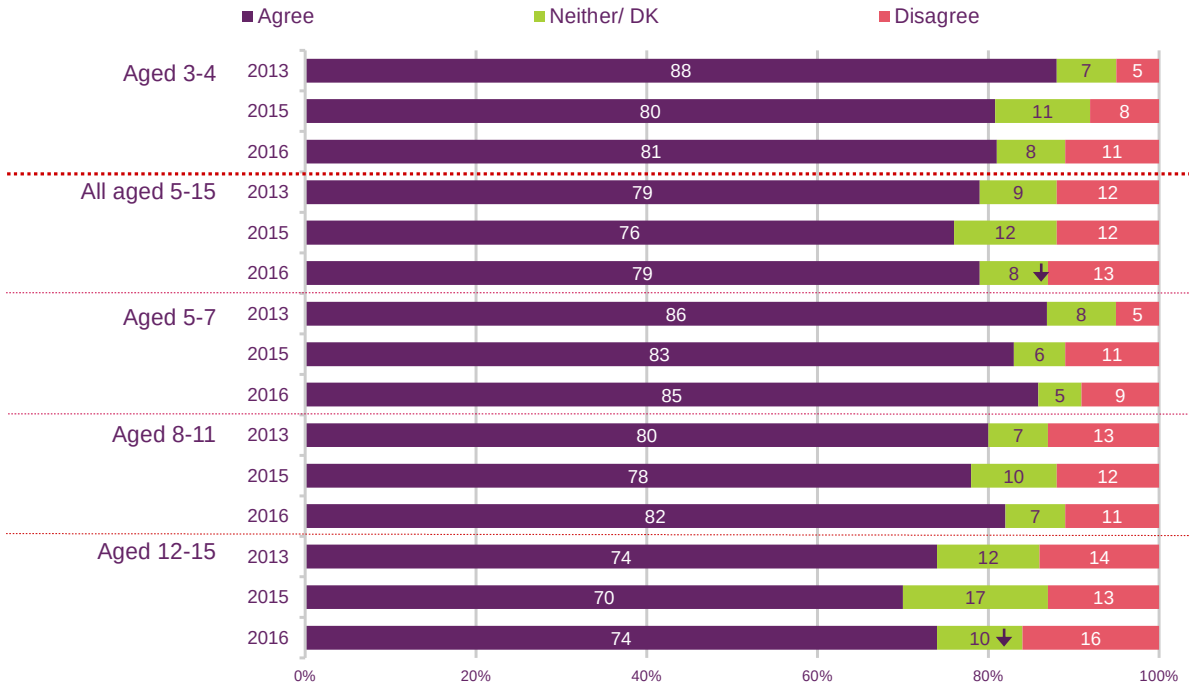
- 81% of parents of 3- to 4-year-olds, 79% of parents of 5- to 15-year-olds and 74% of parents of 12- to 15-year-olds say they know enough to help their children manage online risks (see Figure 29).

However, certain gaps come to light when contrasted with the data regarding parents who think their child knows more about the internet than them:

- only 41% of the parents of 5- to 15-year-olds and 19% of the parents of 12-15 disagree with the statement 'My child knows more about the internet than I do' (see Figure 30).

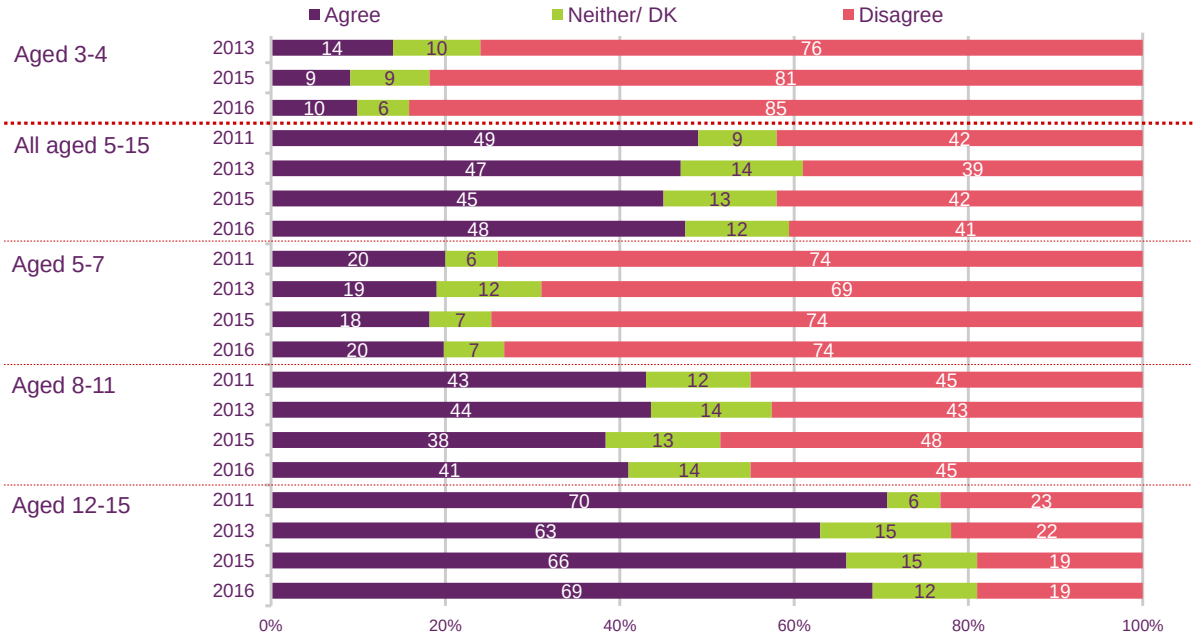
This fits with the data on parents who report that their child shows them new things online and that they learn from them (see Figure 31).

Figure 29: Parental agreement with 'I feel I know enough to help my child to manage online risks*' among those whose child goes online at home (2013), at home or elsewhere (2015, 2016), by age



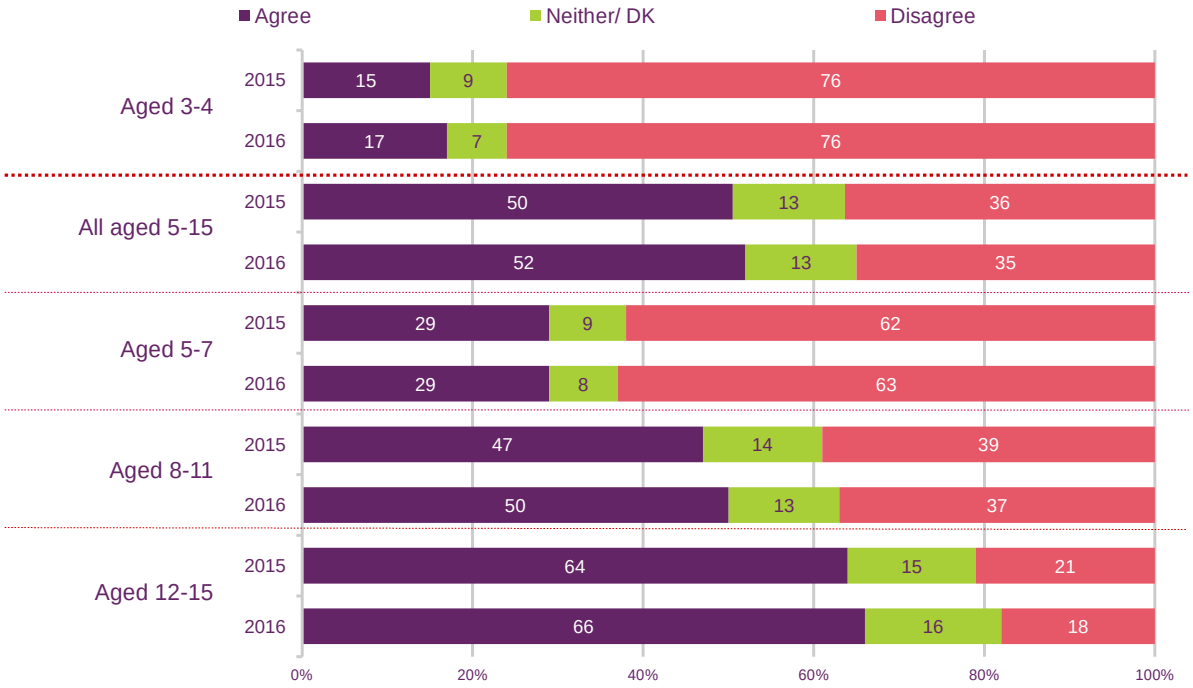
QP48E: Please tell me the extent to which you agree or disagree with these statements in relation to your child (prompted responses, single-coded). * In 2013, this question referred to 'I feel I know enough to help my child to stay safe when they are online'. Base: Parents of children who go online (272 aged 3-4, 1,168 aged 5-15, 264 aged 5-7, 444 aged 8-11, 460 aged 12-15 in 2016). Significance testing shows any difference between 2015 and 2016.
Source: Ofcom (2016a)

Figure 30: Parental agreement with 'My child knows more about the internet than I do' among those whose child goes online at home (2011, 2013) at home or elsewhere (2015, 2016), by age



QP48C: Please tell me the extent to which you agree or disagree with these statements in relation to your child (prompted responses, single-coded). Base: Parents of children who go online (272 aged 3-4, 1,168 aged 5-15, 264 aged 5-7, 444 aged 8-11, 460 aged 12-15 in 2016). Significance testing shows any difference between 2015 and 2016.
Source: Ofcom (2016a)

Figure 31: Parental agreement with 'My child shows me new things online and I learn from them' among those whose child goes online at home or elsewhere, by age, 2015 and 2016



QP48D: Please tell me the extent to which you agree or disagree with these statements in relation to your child (prompted responses, single-coded).
Base: Parents of children who go online (272 aged 3-4, 1,168 aged 5-15, 264 aged 5-7, 444 aged 8-11, 460 aged 12-15 in 2016). Significance testing shows any difference between 2015 and 2016.
Source: Ofcom (2016a)

There are also significant gaps between the availability of information from different sources and parents' preferred source of information:

- According to Table 10 schools are seen as a desirable source of information (and, according to Table 11, they represent the most preferred and accessible source of information for learning about online child safety across all age groups, with ISPs ranking third after families and friends, comprising less than 15% of parents' information sources across all age groups).
- Given that ISPs usually have dedicated safety centres online and readily available open source information and resource guides (see Section 12.6 on industry initiatives), it is worth inquiring into parents' reasoning in favouring one information source over another so as to identify gaps in communicating effective and robust information to parents on their child's online safety.
- For example, awareness-raising campaigns rank quite low in terms of parents' sources of information about their child's online safety. However, for those who were aware of awareness campaigns such as the Safer Internet Day, the majority of the parents (60%) felt that it made them more confident about dealing with online concerns (UK Safer Internet Centre, 2016b).

It will also be useful to disaggregate the data by parents who actively looked for information and those to whom information was conveyed via informal networks or information dissemination campaigns. It is potentially helpful to highlight e-safety best practices among schools and to develop enquiries about the effectiveness of information received via informal networks and the usefulness and uptake of information provided by ISPs online.

Table 10: Parents' perception of what would support their child's online safety

	UK parents say this would contribute…			
	Not at all (%)	Not much (%)	Somewhat (%)	A lot (%)
Guidance in schools	2	7	43	45
Advice for parents	2	12	44	39
Training for parents	5	19	44	28
Parental control software	3	10	42	42
Regulation for businesses	2	8	37	50
Awareness-raising campaigns	2	12	45	37
Helplines	3	18	44	31
Information on consumer rights	4	14	43	35

Q21: To which extent do you think the following would contribute to a safer and more effective use of the internet for your child? (a) More/better teaching and guidance in schools on the commercial activities children/adolescents are exposed to online, (b) More/better information and advice for parents on the commercial activities children/adolescents are exposed to online, (c) Training sessions organised for parents by NGOs, government and local authorities on the commercial activities children/adolescents are exposed to online, (d) Improved availability/performance of parental control software, (e) Stricter regulation for businesses that produce online content and services, (f) More awareness-raising campaigns on online risks, (g) Contact points such as helplines where parents and children can receive individual advice about how to stay safe online, (h) More/better information on consumer rights and the risks of internet cost-traps.
Base: *N*=6,400 parents of 6- to 14-year-olds who use the internet, 800 in each country. UK data only.
Source: Lupiáñez-Villanueva et al. (2016)

Table 11: Parents of 5- to 15-year-olds stating they have looked for or received any information or advice about how to help their child to manage online risks, 2016

All who go online	Aged 3-4	Aged 5-15	Aged 5-7	Aged 8-11	Aged 12-15
Base	272	1168	264	444	460
From child's school	21%	55%	51%	56%	57%
From family or friends	20%	33%	23%	35%	35%
From Internet service providers (ISPs)	12%	14%	13%	13%	15%
From TV, radio, newspapers or magazines	8%	12%	9%	9%	16%
From your child themselves	2%	11%	6%	12%	13%
From other websites with information about how to stay safe online	8%	10%	9%	10%	9%
From Government or local authority	4%	8%	6%	7%	9%
From manufacturers or retailers selling the product	4%	7%	6%	6%	9%
From the BBC	5%	6%	5%	8%	6%
From other sources	1%	3%	2%	3%	3%
TOTAL – ANY INFORMATION LOOKED FOR/ RECEIVED	45%	72%	64%	75%	73%

QP52: Have you looked for or received information or advice about how to help your child manage online risks from any of these sources or in any other way? (prompted responses, multi-coded)
Base: Parents whose child ever goes online aged 3-4 (272) or 5-15 (1,168 aged 5-15, 264 aged 5-7, 444 aged 8- 11, 460 aged 12-15).
Source: Ofcom (2016a)

Parents tend to use the technical controls they are familiar with:

- Parents are more likely to be aware of technical controls such as network-level filters that work effectively on internet services running on HTTP but that fail to be effective against applications installed on smartphones (see Ofcom, 2014b, 2016a).
- Some parents only become aware of parental controls on smartphones after the occurrence of an undesirable incident:

  "… he'd been Googling something on our house computer, and simultaneously on his phone, and something either popped up or he stored something on his phone, I can't remember, and so he'd been looking at porn and obviously we knew how to check his history and stuff. He had no idea that we could do that, ... I said, let's unlock your phone, and let's look at your phone, and he was totally mortified, so we had to go into the shop, because we haven't, when we got his contract phone, we hadn't put any parental settings on it, it just came as it came, and we didn't really know about that." (Alice, teacher/parent of 11-year-old boy) (quoted in Livingstone et al., 2014a, p. 36).

According to Croll (2016), parents might learn to become more adept at parental control tools on mobile phones due to the rapid uptake of mobile phones among children.

12.5 Law enforcement initiatives

A study involving a comparative survey of four EU countries (the UK, Ireland, the Netherlands and Italy) by Davidson et al. (2016) found that cybercrime[35] was so widespread in modern policing that 90.8% of police respondents across all ranks reported dealing with cybercrime at least once on a yearly basis, and emphasised the importance of understanding online child sexual abuse in order to facilitate investigations. The research indicated that the reported incidence of online child sexual abuse (police data) is higher in the UK while the incidence of help-seeking among young people is low:

- While the majority of young people surveyed for the study by Davidson et al. (2016) had not encountered a negative sexual experience online, the UK significantly diverged from the trend, with over half the participants in the UK reporting having being sexually solicited[36] online.
- Less than half the young people in the UK and Ireland sought support when solicited compared to three quarters of young people from Italy.
- Although law enforcement services across the countries surveyed regularly encountered online child abuse cases, it was most marked in the UK.
- Out of online child sexual abuse crimes, UK police officers encounter cases of online grooming and indecent image collection in equal measure.

In the UK online child sexual abuse is largely investigated by specialised units within the police force. The enforcement agency primarily responsible for leading and coordinating the national response to online child sexual abuse is the NCA's CEOP Command. It acts as the UK hub for sex offender intelligence, where reports of abuse from industry, the public and other law enforcement agencies are handled, investigated and disseminated to the relevant local police forces.[37]

[35] Cybercrime here refers to online child exploitation and abuse.

[36] Sexual solicitation here refers to getting in contact with a victim online with the intent to engage in sexual activity.

[37] See www.nationalcrimeagency.gov.uk/about-us/what-we-do/child-exploitation-online-protection-ceop

CEOP's multilateral and multi-agency initiatives provide models of best practice in terms of collaboration. It is part of the Virtual Global Taskforce, a coalition of law enforcement agencies that facilitate transnational law enforcement operations and intelligence.

The CEOP Command's education programme, ThinkUKnow, offers a wide range of information and support for children, young people, parents/carers and professionals, with the aim of developing children and young people's resilience towards the threat of child sexual exploitation and abuse. The programme has a range of resources that have been developed for professionals to use with children and young people aged 5-14+. These materials include films, websites, session plans and practitioner guidance. It also includes the delivery of the CEOP Ambassador course. This cascade-style training provides delegates with the necessary knowledge and materials on child sexual abuse to enable them to deliver a session to fellow professionals within their locality.

CEOP also operates a public reporting mechanism. The 'Click CEOP' button links to an online reporting form where children, young people, parents/carers and professionals can report online grooming or exploitation directly to a team of child protection specialists at CEOP.

CEOP employs a multi-agency approach by joining forces with child protection and education specialists in order to deliver a child-centred operational response and a safe online environment, but there are significant gaps in actual and desired performances in forging key relationships. As can be seen from Table 12, UK ranks lowest in terms of ICT/industry collaboration at 17.3%, which is even lower than the combined average of 22%, although it leads significantly in other key agency collaborations at 70% for education, 40% for charities/NGOs, and, to a lesser extent, at 35.9% for victim support.

Table 12: Collaborations with non-police in dealing with online child sexual abuse

	Country			
	All	**The United Kingdom**	**The Netherlands**	**Italy**
Education	62.0% (N= 431)	70.7% (N= 352)	41.4% (N= 36)	39.1% (N= 43)
Charities / NGO's	35.8% (N= 249)	40.0% (N= 199)	29.9% (N= 26)	21.8% (N= 24)
Victim support	32.4% (N= 225)	35.9% (N= 179)	36.8%(N= 32)	12.7% (N= 14)
ICT/Industry	22.0% (N= 153)	17.3% (N= 86)	47.1% (N= 41)	23.6% (N= 26)
Probation	19.0% (N= 132)	20.5% (N= 102)	31.0% (N= 27)	2.7% (N= 3)
Note. N = number of participants				

Source: Davidson et al. (2016)

Industry can contribute towards advanced training, mentoring and capacity building of specialist police officers as well as the basic training and sensitisation of all rank and file police officers who are usually the first responders. Such collaborative work was found to be ad hoc and infrequent by Davidson et al. (2016).

Joint multi-agency task forces involving specialist law enforcement officers, industry experts and NGOs specialised in working with children can prove effective in the detection and investigation of online child sexual abuse, as well as providing effective victim support to those affected.
In order to facilitate effective coordination and communication with law enforcement it was recommended for the industry to have dedicated points of contact for the police force (Davidson et al., 2016). Out of the police officers surveyed by Davidson et al. (2016), close to 75% believed that improved communication and coordination with industries would help to combat online child sexual abuse.

It is clear that practitioner training, both in understanding young people's use of digital media and in developing effective working practices with young people victimised on social media, is key. Indeed, the recent report by the House of Lords Select Committee on Communications (2017, para. 217) recommended that: 'specific training modules be developed and made compulsory as part of qualifying in frontline public service roles, including but not limited to, police, social workers, general practitioners, accident and emergency practitioners, mental healthcare workers and teachers.'

12.6 Industry initiatives

Just as children and parents have critical and supervisory responsibilities respectively in ensuring a safe internet experience, ISPs can and, to an extent, do play an important role in extending technical and practical controls and tools to their users that enable them to sort through harmful and positive components of the internet. The industry is in a unique position to work alongside educators, parents and carers to facilitate enabling mediation strategies that do not deny children the opportunities while mitigating the risks (see Helsper et al., 2013).

Following an agreement with the government, the UK's four large fixed-line ISPs (BT, Sky, TalkTalk and Virgin Media) committed to offering all new internet customers a family-friendly network-level filtering service by the end of December 2013:

- The filters cover website and social media across a home's internet-connected devices.
- The filters allow users to manage a range of content and contact risks limited to file sharing.
- Filtering categories common to all ISPs include suicide and self-harm, pornography and file sharing, crime, drugs, violence and hate. Some ISPs also offer additional filter categories such as alcohol and tobacco, media streaming, fashion, search engines and portals.

Apart from fixed-line ISPs, industry players such as Vodafone, Facebook and Google have company initiatives and policies towards online child protection: [38]

- ISPs like Vodafone UK rolled out their online child protection filter across their 3G networks in 2004. It also has notice and take-down procedures in place to ensure that illegal content, such as online child sexual abuse images, are promptly removed or dealt with appropriately. There are procedures in place to coordinate with law enforcement agencies on any subsequent investigations. Through their Digital Parenting website and magazine, Vodafone offers parents up-to-date guidance including experts' views on protecting children from online risks as well practical information on how to set up parental controls across a range of internet services and devices.[39] Seventy-nine per cent of the parents surveyed as a part of evaluating the effectiveness of the magazine felt that they were more knowledgeable as a result of it, and 60% have taken action as a result of the magazine, with the majority talking to a partner, their children or their children's teachers (Macleod, 2012).
- Facebook adopts a similar child protection strategy that combines technical and non-technical guidance. Through their Bullying Prevention Hub, developed in partnership with the Yale Center for Emotional Intelligence, it offers targeted information for teens, parents

[38] For information and resources provided by ISPs and tech companies, check the O2 and NSPCC's Internet Safety for Kids online hub (www.o2.co.uk/help/nspcc), Vodafone's Digital Parenting Magazine (www.vodafone.com/content/digital-parenting/learning-and-fun/digital-parenting-magazine.html), Facebook's Bullying Prevention Hub (www.facebook.com/safety/bullying), and Google's Safety Centre (www.google.com/safetycenter/families/start/), among others.

[39] See www.vodafone.com/content/sustainabilityreport/2015/index/operating-responsibly/child-safety-online.html

and educators including how to identify and deal with bullying, step-by-step plans, and how to start some important conversations on the subject.[40]
- Google's Safety Centre offers best practice in having a safe online experience as well as guidance on using a range of safety controls available to parents. The top five safety features include parental controls to filter apps by content rating on Google Play Store, to filter out inappropriate content on YouTube, controlling which sites children can visit via Google Chrome, limiting access to approved apps and games on an android tablet, and family-friendly search results.[41]

Apart from individual company policies, the industry as a whole is making efforts to find industry-level solutions for online child protection. For example, the ICT Coalition is:

- Made up of 20 member organisations working across the ICT sector.
- ICT Coalition members have paid special attention to developing industry consensus on tackling child abuse images online, implementing industry-standard approaches to privacy protection, extensive education and awareness raising, creation of a forum for knowledge exchange, and sharing of experiences between industry partners on internet safety development among others.
- The ICT Coalition operates by a set of six principles relating to content, parental control, dealing with abuse/misuse, child abuse or illegal contact, privacy and control, and education and awareness.[42]

While the industry is pro-actively collaborating to ensure child safety online, due to the evolving nature of technological development, there are still areas that require its collective attention. Although members of the ICT Coalition use recognised content labelling or classification systems, this has not been fully implemented, as a recent independent evaluation shows (O'Neill, 2014). In an assessment made for the ICT Coalition on emerging trends and evolution in IT services, Croll (2016) suggests that:

- The industry should implement platform agnostic content classifications based on consistent standards, and machine-readable labels for user-generated content across all devices.
- There should be user-friendly parental control software especially for apps and websites targeted at small children.
- Developers should be alert to the fact that adding functionalities to devices and services can undermine and potentially compromise their privacy and security.
- Concepts of Safety by Design should rely on artificial intelligence for monitoring inappropriate content and communication.

Other industry coalitions working towards child safety online include GSMA Mobile Alliance Against Child Sexual Abuse Content, founded by a group of international mobile operators to prevent the use of an internet ecosystem from those who consume or profit from child sexual abuse content.[43]

---

[40] See www.facebook.com/safety/bullying

[41] See www.google.com/safetycenter/families/start/

[42] See www.ictcoalition.eu/

[43] Through a combination of technical measures, information sharing and cooperation, the Alliance works towards creating barriers for hosting, accessing and profiting from child sexual abuse content. All Alliance members commit to supporting and promoting 'Hotlines' and other mechanisms for customers to report child sexual content discovered on the internet or mobile content services, enable 'Notice and Takedown' procedures for the takedown of any child sexual content detected on their website, implementing mechanisms to prevent access to websites that have been identified as hosting child sexual content by appropriate agencies (GSMA, n.d.).

However, although professional and policy perspectives celebrate the effectiveness of technical solutions like home network-level filters, it was found that these were largely ineffective in a study by Przybylski & Nash (2017). Specifically, children living in households with the filters on reported equivalent exposure to online risk to those in households with the filters off, perhaps because children access the internet from elsewhere as well as at home.[44]

12.7 Building digital resilience

In their study exploring how children and young people can be supported on the internet, Przybylski et al. (2014, p. 4) understand resilience to be an:

> … individual's ability to accurately adapt to changing and sometimes stressful environments and to feel empowered to act instead of react in the face of both novel and threatening challenges.

Thus, in order to develop this capability in children, it is not ideal to have overtly restrictive mediation strategies in children's lives seeking to nullify all risk involved, but instead, a system of enabling mediation that attempts to develop the critical capability in children for risk recognition and adequate self-regulation as well as skills for mitigating the online risks encountered. However, children can best learn to face and cope with a degree of risk in a supportive and sympathetic context that allows them to feel safe and not harshly judged if they make mistakes. Such a context should be provided both at home and in school, as well as in the digital environment itself.

It is important to develop digital resilience because children can thereby live as active agents in their own right, able to exercise self-control and independent judgement:

- Children's perception and management of risks differ significantly from that of adults (Vandoninck, d'Haenens, & Smahel, 2014; see also Children's Commissioner, 2017).
- Children's perception of risk will depend on their assessment of the online environment and its possible consequences, including knowledge of opportunities for support and redress.
- Parental mediation strategies and the technical tools available are overwhelmingly skewed toward addressing content-based risk, with less focus on issues such as cyberbullying, grooming, sexting and online harassment.

Efforts to develop children's digital resilience should focus on critical ability and technical competency in order to support children in becoming active agents in their own protection and safety:

- Building digital resilience is aimed at strengthening the ability of the child to correctly identify and interpret the impact and repercussions of the various online risks, and to develop both the technical and emotional competencies to deal with them.
- Thus it requires building their knowledge and awareness around the entire gamut of online risks without focusing exclusively on particular or immediate risks.
- Vandoninck, d'Haenens and Smahel (2014) found that when children feel capable of dealing with a risk, they are less likely to be fearful or worried by it.

By helping children to become more confident and competent users of the internet, including being able to face and deal with online risks, they will be able to embrace more online opportunities without needing to be curtailed by restrictive mediation strategies.

[44] This was a correlational (cross-sectional) analysis of Ofcom's data. A more robust test of filter effectiveness on childhood experiences and outcomes would require a longitudinal and experimental study.

Building digital resilience is more urgent than ever because an increasing number of risky activities are being perpetrated through social media platforms that parents and teachers have limited ability to regulate (see Sections 12.2-12.4). Increased time spent online means that children are continuously presented with moral and ethical choices as content producers and consumers (Day, 2016), and are already active decision-makers in the process. Attempts to build children's digital resilience should be based on a child-centred approach by:

- leveraging these skills
- promoting increased awareness of the consequences of certain activities
- parents, educators and policy-makers giving credence to young people's online experiences and risk and opportunity environments so that future strategies unlock children's agency in creating online child protection frameworks that are more closely related to children's lived experiences.

Thus, building digital resilience requires a multistakeholder approach that includes children's voices in the formulation of effective policies targeting their own online safety.

Figure 32: Multistakeholder approach to cyberbullying

This figure (from a Boston Consulting Group and Telenor Group study) breaks down the constituting components of building digital resilience capabilities in children as per the stakeholders responsible for implementing them.[45]

[45] From www.telenor.com/wp-content/uploads/2013/04/Telenor-report-Building-Digital-Resilience.pdf

12.8 Summary

Regarding safeguarding children online:

- The overwhelming picture is that while many initiatives have been tried by diverse stakeholders, very few are independently evaluated. This makes it difficult to determine what works and why. Such evaluations as are undertaken tend to focus on immediate outcomes (reach, appeal, etc.) rather than a long-term reduction in harm or improvement in wellbeing.
- Schools use a range of strategies to implement e-safety priorities – including developing children's critical abilities - but there is mixed evidence of improvement.
- Awareness-raising campaigns such as a Safer Internet Day have been instrumental in changing attitudes and practices.
- Parents use a range of mediation strategies including technical controls, rules regulating online access and use, with the majority preferring to talk to their children about the consequences of their online activities – but gaps remain in parents' abilities and skills for effective mediation; rules and restrictions tend to keep children safe but constrain their opportunities and invite evasion; enabling mediation is empowering providing children and parents have the skills and resilience to cope with risk when it occurs.
- Parents prefer to receive information about their children's online safety from schools despite information being available from multiple sources.
- Parents tend to prefer control tools they are familiar with unless an undesirable incident prompts them to adopt a new one.
- Industry initiatives exist in the form of agreements with the government, individual company policies and initiatives, and industry-level initiatives (such as the ICT Coalition and GSMA Mobile Alliance Against Child Sexual Abuse).
- Building children's digital resilience should have a twin focus on developing critical ability and technical competency in terms of education, as well as supporting children online and offline through constructive and informed parenting practices, through safety and privacy by design, and by improving the digital expertise of relevant welfare and other professionals who work with children.
- There are some examples of good industry and law enforcement collaboration in the UK, but this practice is ad hoc. There is a need to develop a central platform to enable and encourage a collaborative approach in investigation and joint training that is standardised and based on current research evidence.

13. Conclusions

The UKCCIS focuses on developing evidence-based strategies to reduce or manage online risks of harm to children. To this end, it seeks to guide relevant stakeholders – government, industry, educators, welfare providers, parents and children themselves – in playing their parts as best they can. In this section we identify the main findings of our evidence review in order to inform UK policy and practice regarding recent developments, identify emerging issues and the related implications for children's online risk and safety.

13.1 Children's internet use

Most of this review has focused on risk and safety. However, we begin by noting the changing ways in which children go online, as this provides the context for online risk, and also explains children's motivations and the anticipated benefits of their internet use. Key findings regarding children's use of the internet include the following:

- The majority of children aged 5-10, and nearly all 11- to 16-year-olds, now use the internet, as do around one in three 3- to 4-year-olds. While the proportion of internet users aged 5+ appears to have reached a plateau, it is possible that more pre-school children will use the internet in the coming years.
- The overall amount of use among internet users continues to rise year on year, with no evidence of reaching a limit.
- Inequalities in access and use are too little studied, but there is evidence that the poorest households have access to fewer devices, and a minority of children lack consistent/affordable connectivity.
- The range of activities children undertake online increases with age, and the nature of their activities and interests also alters, with more communication, learning and content creation among older children – although more advanced creative and civic activities are only practised by a minority.

While there appears to be considerable scope to increase the beneficial uses of the internet among UK children, there is heartening evidence that children are taking relatively few risks in their online behaviour:

- Few add online contacts they don't know or send photos of themselves they later regret, and most appear to have learned not to disclose personal information online.
- Other forms of risky online behaviour are more common – around a quarter of 8- to 12-year-olds use SNSs 'under age', and there is a fair degree of experimentation among teens with multiple social media sites or apps.

13.2 Assessing online risk

While the above statistics are generally accepted, there is more uncertainty regarding evidence of online risk. The frequency with which children encounter online pornography, whether online hostility is interpreted as bullying or shrugged off, or whether an approach by a stranger results in a child sending an indecent image – these and other risk encounters cannot easily be measured except by asking children directly:

- This raises ethical questions – researchers aim not to introduce knowledge of risk to children who are hitherto unaware, and must have the means to address any harms that they uncover.

- It also raises measurement questions – embarrassment or social desirability pressures may make it likely that children will under-estimate risk, although the desire to brag or 'fit in' may also lead them to over-estimate when they report risk. Other measurement issues concern ways of describing risk – do children mean what adults mean by pornography, bullying or violence, for instance?[46]

We stress these uncertainties by way of explaining the range of estimates of risk produced across different studies:

- In general, studies conducted using sampling that is representative of the UK population, and studies that take care with measurement and research ethics, tend to produce lower estimates than some of the so-called 'polls' or 'anecdotal evidence' or ad hoc surveys reported in the popular media.
- Further, all research apart from that focusing on 'at risk' children or those from specifically marginalised subgroups is likely to under-represent them and, potentially, underestimate the incidence of online risk to, for instance, children who are migrants, have a disability, are in care or are otherwise disadvantaged.

We conclude that more UK children are aware of the internet as a source of risk than have personally encountered risks. This in itself has consequences for children's perception of the online world, potentially undermining their confidence to explore freely online:

- Since adolescence is crucially a time of exploration and experimentation, and since the internet provides an opportunity for such exploration that adolescents value, this is significant. As we have noted earlier, resilience cannot develop in a risk-free, overly-cautious environment.
- It also matters because research is not able to predict which children will experience harm as a result of encountering risk. After all, risk refers to the probability of harm, since encountering hostile messages or pornographic images is not necessarily harmful. It is also important to consider the severity of harm – some risks may be rare but severe in their consequences, and this, too, is difficult to assess.

In the discussion of vulnerability, we note some of the factors that emerging research suggests are likely to result in some young people being less resilient to online risks, for example:

- children who experience family difficulties or who are brought up in chaotic family/home environments
- children who suffer physical, emotional and/or sexual abuse and neglect, witness domestic violence and/or family breakdown
- children brought up in an environment in which drugs and alcohol abuse of the adults around them impinges on the quality of parenting they receive. They may also be children who, having been judged to have suffered significant harm, are placed in the care system.

We also noted that while there are some very good general internet safety awareness programmes such as those run by CEOP (e.g., ThinkUKnow) and Childnet, there appears to be a lack of research exploring practice approaches with vulnerable children and young people online, with the exception of research by Palmer et al. (2015). This review also identified the urgent need for comprehensive practitioner training (e.g., child safeguarding professionals and law enforcement) in

[46] It is also important to consider the exact questions asked of children – many children report awareness of online risks, or knowledge that a friend or peer has encountered a particular risk. Fewer say they have encountered a risk personally, even fewer say they have encountered a risk online in recent months, and yet fewer say that they have been upset about or concerned by such experiences. Researchers tend to use different terms to refer to online risks, and thus we include where possible the exact phrasing when reporting findings.

assessing and working with children and young people experiencing online harm, as well as in understanding their use of digital media.

Knowledge in respect of online vulnerability is, however, far from complete, particularly in the UK, and since children are no more homogeneous than the adult population, a host of factors affect the distribution of risk and harm, vulnerability and resilience.

13.3 Platforms, games and risk

As observed earlier, Ofcom's (2016a) survey of children aged 8-15 found that 2% of those aged 8-11 and 12-15 reported being bullied via online games, while around 2% of 8-11 year olds and 6% of 12-15 year olds reported being bullied via social media.

EU Kids Online's analysis of where children said they found the content, contact or conduct that bothered them online revealed that video-sharing sites came top (32% of reported risk), followed by websites (29%), then SNSs (13%) and games (10%) (Livingstone et al., 2014b).

There is some evidence that gaming is becoming a pathway to illegal activity – hacking and also radicalisation (see earlier).

Games may also be riskier for vulnerable children such as those with special educational needs insofar as they find it difficult to judge what is real or to read the intentions behind an approach by other players.

In the main, the specific nature of the platforms or game environments in which children encounter online risk has been little studied, making this a key evidence gap for future research.

13.4 The importance of age in relation to risk

In addition to the question of specific risk factors, children's age is a major factor influencing their online experiences. We summarise the findings by age by drawing on the work of Dr Angharad Rudkin, who summarised the process of child development for the UKCCIS report, *Child safety online: A practical guide for providers of social media and interactive services*.[47] In Table 13 we have retained (albeit slightly paraphrasing) her original account of children's overall development and attitudes to risk. We have added a summary of the findings regarding children's online activities and experiences of risk and safety, based on the evidence reviewed.

[47] Available on page 53 of www.gov.uk/government/uploads/system/uploads/attachment_data/file/517335/UKCCIS_Child_Safety_Online-Mar2016.pdf. This summary is supported by expert accounts of child development, including from neuroscience.

Table 13: Age and risk factors

Age	Development
3- to 5-year-olds	They can put themselves in others' shoes, but are still quite fooled by appearances. They are beginning to learn that there are social rules to follow, and are starting to build up friendships. Peer pressure remains low, as, however, is awareness of online risks. Around four in ten UK 3- to 4-year-olds use the internet, going online for around 8 hours per week on average, often via a tablet computer, and they like to watch videos on YouTube. At this age, children may be vaguely aware that there may be problems with internet use, but understanding is very limited. There are also rising privacy concerns regarding their parents' activities in posting images of them.
6- to 9-year-olds	Their play is mainly pretend/role-play, moving towards greater rule-based reality play. It is becoming socially more sophisticated, and the need to fit in and be accepted by the peer group is becoming more important. They are learning how to manage their thinking and their emotions, and about the complexities of relationships; if they can't manage these it can lead to alienation, bullying and loneliness. At around 7, they undergo a significant shift in thinking to more order and logic. They tend to comply with messages from school/home – although if risks aren't explained clearly, they imagine their own explanations. Two thirds of 5- to 7-year-olds go online, rising to nine in ten 8- to 11-year-olds, with average hours per week for these age groups rising from nearly 9 to near 13 hours per week. Games and watching videos are the favourite activities. They encounter considerably less online risk than older children and teenagers, but are easily upset when they encounter hostility, pornography or other online risks. Fewer than one in ten say that they encountered something online that was worrying or nasty in the past year. They can be upset by online nastiness, approaches from strangers, videos showing violence or cruelty, among other things.
10- to 13-year-olds	They are moving towards more adult ways of thinking, but are still not making decisions the way adults would. They are very aware of social pressure and expectations, and will change aspects of themselves in order to fit in and be accepted by peers. Friends are becoming more important, and they are more aware of what's 'cool' or not, including brands. Girls show a decrease in self-esteem as they compare themselves to others around them. Developmentally, the strong desire for immediate rewards triggers risk-taking behaviour. All but a small minority now use the internet, with time online for 12- to 15-year-olds averaging 20 hours per week. Videos and music are the favoured activities, with a growing interest in messaging friends and family. This group is beginning to explore more independently online, and the start of secondary school marks a key shift in use of digital and social media to build new peer networks and to explore new social and relationship possibilities, potentially leading to risky encounters. Online behaviour many remain cautious, still respectful of parental warnings, although some see the internet as a fun space for transgressive exploration and risk-taking. Some, further, find it suits their particular identity or emotional needs to meet others and share experiences in new ways.
14- to 18-year-olds	They are undergoing significant neuro-psychological changes, leading to differences in the way they perceive emotions and make decisions. Developments in the pre-frontal cortex may contribute to the increase in risk-taking behaviour seen during adolescence. Mental health difficulties such as anxiety and depression can intensify.

They still have difficulties realising that others can have a different perspective, so may find it hard to work out interpersonal problems. Adolescence is a time characterised by idealism, with a tendency towards all-or-nothing thinking. They are highly dependent on peers for a sense of wellbeing, needing to feel as if they are part of a group – yet also wanting to be viewed as unique. They can appear to shun adult influence but still require clear boundaries and support from parents and teachers. Visual communication is now vital and the 'currency' of likes and ratings is very important. They are more settled within peer groups and are getting better at the risk/reward equation.

Ninety-eight per cent use the internet, with time online for 12- to 15-year-olds averaging 20 hours per week, preferring the smartphone but using a range of devices across home, school and elsewhere. Music, messaging and social networking are the favourite activities.

As they get older, becoming more independent online and offline, they encounter more risk online – in terms of breadth of risks, severity and frequency. Still, fewer than one in five 12- to 15-year-olds said they encountered something worrying or nasty online in the past year. While this age group encounters most risk, they also have the most skills, coping strategies and resilience to cope, on average. However, there are significant exceptions and vulnerabilities (with online vulnerabilities generally explained by similar factors to those that account for offline vulnerability and risk). This is a period also characterised for some by mental health disorders, substance misuse and problematic relationships. This group is also becoming familiar with a more adult internet in which hostility, hate, sexual risks and other problems are commonplace, known about and discussed as occurring to peers, if not so often experienced personally.

13.5 Gendered dimensions of online activities, risks and safety

Since online victimisation often tends to follow offline patterns of targeting and abuse, it is important to understand how children's gender and identity influence their online use and risk environments. The following is a summary of the relationship between gender and these contexts, as well as the incidence of online risks for children:

- *Children's use of the internet:* there are no significant gender differences in relation to access to digital media and the internet. However, girls tend to report fewer skills than boys.
- *Children's online activities:* girls are less likely to 'be themselves' online than boys (74% vs. 92%). This gap is greater than the gap between other discriminated against groups such as children with disabilities (69% vs. 79%). Girls are also more likely to offer positive reinforcement to their peers online than boys (58% vs. 35%).
- *Risk of harm to children online:* the EU Kids Online qualitative research by Livingstone et al. (2014b) found that boys are more likely to be concerned about violent content online while girls are more concerned about contact and conduct-related risk.
- *Bullying, aggression and hate:* girls are more likely than boys to report victimisation online or by phone, particularly that which has a gendered or sexual dimension.
- *Sexting and sexual harassment:* girls are more likely to be pressurised to send sexual images (27% vs. 7%) and report non-consensual sharing of their images (41% vs. 13%). There is evidence that offline patterns of sexual harassment are replicated online. This includes unwanted sexual attention, judgements about appearance and sexual behaviour, as well as being targeted with sexual and insulting language.
- *Pornography:* there are significant differences in gender with regard to exposure and attitudes towards pornography. Double the number of girls compared to boys believe pornography leads

to unrealistic attitudes about sex (40% vs. 21%) and encourages society to view women as sex objects (37% vs. 18%).
- *Grooming, child sexual abuse and exploitation:* studies conducted in Canada and the UK show that close to two thirds of the victims are girls.
- *Online radicalisation:* there are no significant relationships between gender and victimisation in this area.
- *Hacking:* hackers are more likely to be male.

It is important to develop an understanding of the gendered dimensions of children's online activities and risk environments in order to develop targeted and gender-responsive policy-making in these areas. The guidance document developed by UKCCIS (2016) in partnership with key stakeholders is a positive step in proposing a safeguarding approach to sexting, with an emphasis on the non-criminalisation of children.

However, it is important to revisit the gendered dimensions of the behaviour, particularly as they relate to the role of coercion and related responses in the context of the peer groups of those involved. Peer pressure is often reflective of entrenched gender stereotypes, as reflected in the gendered expectations and judgements around sexting. There is evidence of a double standard in which girls feel pressured by boys to engage in the behaviour, but those who do are often judged negatively by their male and female peers. Similar judgements do not appear to be made of boys who send sexual images, although the influence of gendered expectations and roles are evidenced by peer pressure to be sexually active and 'laddish', which may also result in harmful experiences.

The Insafe helplines' evaluation (Dinh et al., 2016) found that more calls are received from girls than boys across the majority of organisations examined, with a marked reduction in volume of calls received from boys of 17% from the previous year. This is likely to reflect gendered expectations that lead boys to feel the need to appear tough and in control, regardless of any problems they might be experiencing.

These issues indicate the importance of developing gender-sensitive awareness programmes aimed at fostering positive gender attitudes among children in both the online and offline environment. Existing internet safety educational resources, for example, CEOP's ThinkUKnow programme, which are already making an impact in raising awareness among children and other stakeholders, should also address online behaviours and experiences that are rooted in entrenched gender norms and practices. It would also be helpful to develop resources and guidance for children that explore these issues in the context of recognising suspicious behaviour and potentially harmful activities.

There is also a need to develop support systems that vulnerable children can access when they feel threatened, and recognition of the potentially gendered expectations and experiences that may be involved and influence help-seeking behaviour. It is important to recognise that attempts to address online sexual harassment and other gendered experiences online cannot be examined without consideration of their wider social and cultural contexts.

13.6 Safeguarding initiatives and good practice

- Digital literacy is vital for children to benefit from online opportunities and to safeguard themselves from the risk of harm. Children's digital literacy develops in nature and degree as they grow up, but it is marked by some significant gaps in understanding in relation to the digital environment, especially as this translates into behaviour online, and there is little evidence of improvement in recent years.
- The role of schools is important in teaching critical digital literacy to students, as well as in guiding and informing parents regarding children's internet use at home. There are challenges,

however, in ensuring teachers are sufficiently trained and up to date in their knowledge, in promoting critical understanding rather than restrictive approaches to safety, as well as in tasking schools with guiding students and parents in their use of the internet at home.

- Nearly all parents report undertaking one or more activities to support and safeguard their child(ren) online, employing a mix of enabling and restrictive strategies depending on their parenting style and their digital skills. Parents are more concerned about online content and online privacy the older their child. Although most know of parental control software (in terms of ISP filters, less so for safety settings on phones or tablets), most do not use them – although those who do say they have found them helpful and are confident their child cannot get around them. While most parents have discussed managing online risks with their children, one in ten with children aged 8-15 have not done so (and this has changed little in recent years).
- Only one in five parents say they do not know enough to help their child manage online risks, although most consider that their child knows more about the internet than they do and many, too, learn about the internet from their child. They would most like to get advice from schools – for themselves and their child. Parents also call for stricter regulation for business and better parental control software, among other initiatives. Only around half, however, have looked for or received advice from their child's school, and few look to other sources.
- Cybercrimes against children are becoming a frequent focus for law enforcement, requiring a mix of awareness raising, policing strategies and effective collaboration with industry and other key stakeholders.
- Industry providers operate a mix of approaches to child internet safety, including awareness raising, notice and take-down procedures, parental controls and guidance, child support hubs, filters and more. There are also efforts to coordinate and cooperate across providers to create a safer digital environment overall. Content labelling remains a challenge, however, as does the provision of filters that effectively reduce exposure to risk of harm. Transparency in responding to children's concerns is a further challenge as is working more effectively with law enforcement and other criminal justice agencies.
- Efforts to support digital resilience tread a fine line between allowing children to encounter risk in order to develop constructive coping strategies and avoiding undue risk of harm for children who are vulnerable or otherwise unready to face such risks. Support is growing for initiatives that can build digital resilience in children, but they are yet to be available to children nationally or to be independently evaluated.
- There is an ongoing need to ensure that those practitioners involved in the investigation and prosecution of online child abuse cases, and those involved in addressing the therapeutic and welfare needs of young victims of online abuse, have at least a basic understanding of children's use of digital media and key current research findings that should inform their practice from initial assessment.

14. Sources cited

Aiken, M., Davidson, J., Amann, P. (2016). *Youth pathways into cybercrime*. London. Retrieved from www.paladincapgroup.com/wp-content/uploads/2016/11/Pathways-White-Paper-US-final-1.pdf.

Aiken, M., Moran, M., & Berry, M. J. (2011). Child abuse material and the internet: Cyberpsychology of online child related sex offending. *29th Meeting of the INTERPOL Specialist Group on Crimes against Children* (pp. 1-22). Lyon: INTERPOL.

Aston, H., & Brzyska, B. (2012). *Protecting children online: Teachers' perspectives of e-safety*. Retrieved from www.nfer.ac.uk/publications/95001/95001.pdf.

Bailey, P. (2015). *Guidance for working with children and young people who are vulnerable to the messages of radicalisation and extremism*. London Borough of Merton, Merton Safeguarding Children Board. Retrieved from www.merton.gov.uk/mscb_prevent_guidance_final.pdf.

Belton, E., & Hollis, V. (2016). *A review of the research on children and young people who display harmful sexual behaviour online*. Retrieved from www.nspcc.org.uk/globalassets/documents/research-reports/review-children-young-people-harmful-sexual-behaviour-online-large-text.pdf.

Bergen, E., Davidson, J., Schulz, A., Schuhmann, P. Johansson, A., Santtila, P., et al. (2014). The effects of using identity deception and suggesting secrecy on the outcomes of adult-adult and adult- child or -adolescent online sexual interactions. *Victims & Offenders, 9*(3), 276-298.

Biddle, L., Gunnell, D., Owen-Smith, A., Potokar, J., Longson, D., Hawton, K., et al. (2012). Information sources used by the suicidal to inform choice of method. *Journal of Affective Disorders, 136*, 702-9.

Bizina, M., & Gray, D. H. (2014). Radicalization of youth as a growing concern for counter-terrorism policy. *Global Security Studies*, *5*(1). Retrieved from www.globalsecuritystudies.com/Bizina%20Youth-AG.pdf.

Bond, E. (2012). *Virtually anorexic – Where's the harm? A research study on the risks of pro-anorexia websites.* Retrieved from www.nominettrust.org.uk/sites/default/files/Virtually%20Anorexic%20-%20Where%27s%20the%20harm.pdf.

Bond, E., Agnew, S., & Phippen, A. (2014). *The Children's Workforce across England is ill-equipped to meet the needs of child victims of online abuse*. Retrieved from www.mariecollinsfoundation.org.uk/mcf/news/the-childrens-workforce-across-england-is-ill-equipped-to-meet-the-needs-of-child-victims-of-online-abuse.

Buckingham, D. (2007). Digital media literacies: Rethinking media education in the age of the internet. *Research in Comparative and International Education, 2*(1), 43-55.

Buckingham, D., Banaji, S., Burn, A., Carr, D., Cranmer, S., & Willet, R. (2004). *The media literacy of children and young people: A review of the research literature on behalf of Ofcom*.

London: University of London. Retrieved from http://eprints.ioe.ac.uk/145/1/Buckinghammedialiteracy.pdf.

Byron Review (2008). *Safer children in a digital world.* Nottingham: Department for Children, Schools and Families and the Department for Digital, Culture, Media and Sport.

Cafcass. (2016). Study of data held by Cafcass in cases featuring radicalisation concerns. Retrieved from www.cafcass.gov.uk/media/286999/cafcass_radicalisation_study__external_version_.pdf.

Carrick-Davies. S. (2011). *Munch poke ping! Vulnerable young people, social media and e-safety.* Retrieved from www.carrick-davies.com/downloads/Munch_Poke_Ping_-_E-Safety_and_Vulnerable_Young_People_FULL_REPORT.pdf.

CEOP (Child Exploitation and Online Protection Centre) (2013). *Threat assessment of child sexual exploitation and abuse.* Retrieved from https://ceop.police.uk/Documents/ceopdocs/CEOP_TACSEA2013_240613%20FINAL.pdf.

CEOP (n.d.). *E-crime reduction partnership – Online child protection*. Retrieved from www.eurim.org.uk/activities/e-crime/CEOP_Briefing.pdf.

Chen, Y-Y., Bennewith, O., Hawton, K., Simkin, S., Cooper, J., et al. (2013). Suicide by burning barbecue charcoal in England. *Journal Public Health*, 35, 223-7.

Children's Commissioner (2017). *Growing up digital: A report of the growing up digital taskforce.* Retrieved from www.childrenscommissioner.gov.uk/sites/default/files/publications/Growing%20Up%20Digital%20Taskforce%20Report%20January%202017_0.pdf.

Childwise (2017). *Monitor report 2017: Children's media use and purchasing.*

Clarke, B., & Crowther, K. (2015). *Children internet safety report: Key findings.* Family Kids and Youth, Techknowledge for schools.

Cooper, K., Quayle, E., Jonsson, L., & Svedin, C. G. (2016). Adolescents and self-taken sexual images: A review of the literature. *Computers in Human Behavior, 55*, 706-16.

Corb, A., & Grozelle, R. (2014). A new kind of terror: Radicalizing youth in Canada. *Journal Exit-Deutschland, 1*, 32-58.

CREST (2015). *Identify, intervene, inspire: Helping young people to pursue careers in cyber security, not cyber crime*. London. Retrieved from www.crest-approved.org/wp-content/uploads/CREST_NCA_CyberCrimeReport.pdf.

Croll, J. (2016). *Let's play it safe: Children and youth in the digital world.* ICT Coalition. Retrieved from www.ictcoalition.eu/gallery/100/REPORT_WEB.pdf

d'Haenens, L., Vandoninck, S., & Donoso, V. (2013). *How to cope and build online resilience.* Retrieved from http://eprints.lse.ac.uk/48115/1/How%20to%20cope%20and%20build%20online%20resilience%20(lsero).pdf

Daine, K., Hawton, K., Singaravelu, V., Stewart, A., Simkin, S., et al. (2013) The power of the web: A systematic review of studies of the influence of the internet on self-harm and suicide in

young people. *PLoS ONE, 8*(10). doi:10.1371/journal.pone.0077555

Davidson, J., DeMarco, J., Bifulco, A., Bogaerts, S., Vincenzo, C., Aiken, M., et al. (2016). *Enhancing police and industry practice: EU Child Online safety project*. London. Retrieved from www.mdx.ac.uk/__data/assets/pdf_file/0033/248469/EU_Child_Online_Safety_Project.pdf.

Day, L. (2016). *Resilience for the digital world: Research into children and young people's social and emotional well-being*. YoungMinds and Ecorys. Retrieved from www.youngminds.org.uk/assets/0002/5852/Resilience_for_the_Digital_World.pdf.

Del Rey, R., Casas, J.A., & Ortega, R. (2016). Impact of the ConRed program on different cyberbulling roles. *Aggressive Behavior*, *42*(2), 123-35. doi:10.1002/ab.21608.

DfE (Department for Education) (2014). *Preventing and tackling bullying: Advice for headteachers, staff and governing bodies*. Retrieved from www.gov.uk/government/uploads/system/uploads/attachment_data/file/444862/Preventing_and_tackling_bullying_advice.pdf.

DfE (2015). *The Prevent duty: Departmental advice for schools and childcare providers*. London.

DfE (2017). *Child sexual exploitation: Definition and guide for practitioners, local leaders and decision makers working to protect children from child sexual exploitation.* Retrieved from www.gov.uk/government/uploads/system/uploads/attachment_data/file/591903/CSE_Guidance_Core_Document_13.02.2017.pdf.

Dinh, T., Farrugia, L., O'Neill, B., Vandoninck, S., & Velicu, A. (2016). *Insafe helplines: Operations, effectiveness and emerging issues for internet safety helplines*. European Schoolnet, Insafe, EU Kids Online, & Kaspersky Lab. Retrieved from http://eprints.lse.ac.uk/65358/.

Ditch the Label (2013). *Annual cyberbullying survey.* Retrieved from www.ditchthelabel.org/wp-content/uploads/2016/07/cyberbullying2013.pdf.

Edwards, C. & Gribbon, L. (2013). Pathways to violent extremism in the digital era. *The RUSI Journal*, *158*(5), 40-7. doi:10.1080/03071847.2013.847714.

Elzinga, P., Wolff, K. E., & Poelmans, J. (2012). Analyzing chat conversations of pedophiles with temporal relational semantic systems. In *2012 European Intelligence and Security Informatics Conference* (pp. 242-9). IEEE. Retrieved from http://doi.org/10.1109/EISIC.2012.12.

European Parliament. (2011). *Directive of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA* (PE-CONS 51/11). Brussels, Belgium: European Parliament and the Council of the European Union. Retrieved from http://register.consilium.europa.eu/doc/srv?l=EN&f=PE%2051%202011%20INIT.

Europol. (2014). *Europol iOCTA: Threat assessment on internet facilitated organised crime*. The Hague. Retrieved from www.europol.europa.eu/content/publication/iocta-threat-assessment-internet-facilitated-organised-crime-1455.

Family Kids & Youth. (2016). *Research into the attitudes of 1-16 year olds.* London: Family Kids & Youth for The Royal Foundation of the Duke and Duchess of Cambridge and Prince Harry.

Family Kids & Youth. (2017). *Cyberbullying: Research into the industry guidelines and attitudes of 12-15 year olds*. London: Family Kids & Youth for The Royal Foundation of the Duke and Duchess of Cambridge and Price Harry.

Ferguson, C.J. & Heene, M. (2012). A vast graveyard of undead theories: Publication bias and psychological science's aversion to the null. *Perspectives on Psychological Science*, *7*(6), 555-61. doi:10.1177/1745691612459059.

FOSI (Family Online Safety Institute). (2012). *The online generation gap – Contrasting attitudes and behaviours of parents and teens*. Retrieved from http://safekids.com/pdfs/fosireport2012.pdf.

Geeraerts, S. B. (2012). Digital radicalization of youth. *Social Cosmos, 3*(1), 25-32.

Gill, P., Corner, E., Thornton, A., & Conway, M. (2015). *What are the roles of the internet in terrorism? Measuring online behaviours of convicted UK terrorists*. London: VoxPol. Retrieved from www.voxpol.eu/download/report/What-are-the-Roles-of-the-Internet-in-Terrorism.pdf.

Girlguiding UK (2014). *Girls' attitude survey 2014.* Retrieved from www.girlguiding.org.uk/globalassets/docs-and-resources/research-and-campaigns/girls-attitudes-survey-2014.pdf.

GSMA (n.d.). *Mobile alliance against child sexual abuse content*. Retrieved from www.gsma.com/publicpolicy/wp-content/uploads/2013/10/GSMA_The-Mobile-Alliance-Against-Child-Sexual-Abuse-Content_Oct-2013_2ppWEB.pdf.

Gunnell, D., Coope, C., Fearn, V., Wells, C., Chang, S-S., Hawton, K., et al. (2014). Suicide by gasses in England and Wales 2001-2011: Evidence of the emergence of new methods of suicide. *Journal of Affective Disorders, 170*, 190-5.

Harris, L. (2015). Rise in child and teen fraud arrests mainly due to increase of internet-based crimes. *Daily Telegraph*. Retrieved from www.dailytelegraph.com.au/news/nsw/rise-in-child-and-teen-fraud-arrests-mainly-due-to-increase-of-internetbased-crimes/news-story/fc620acdb8379e30ab46f17493e40475.

Helsper, E.J., Kalmus, V., Hasebrink, U., Sagvari, B., & De Haan, J. (2013). *Country classification: Opportunities, risks, harm and parental mediation*. London: EU Kids Online, London School of Economics and Political Science. Retrieved from http://eprints.lse.ac.uk/52023/.

Hinduja, S. & Patchin, J. W. (2010). Bullying, cyberbullying, and suicide. *Archives of Suicide Research, 14*(3), 206-21. doi:10.1080/13811118.2010.494133.

Horvath, M. A. H., Alys, L., Massey, K., Pina, A., Scally, M., & Adler, J. R. (2013). *'Basically ... porn is everywhere': A rapid evidence assessment on the effects that access and exposure to pornography has on children and young people*. Retrieved from http://eprints.mdx.ac.uk/10692/1/BasicallyporniseverywhereReport.pdf

House of Commons. (2016). *Radicalisation: The counter-narrative and identifying the tipping point. Eighth Report of Session 2016-17*. Retrieved from www.publications.parliament.uk/pa/cm201617/cmselect/cmhaff/135/135.pdf.

House of Lords. (2017). *Growing up with the internet. 2nd report of session 2016-17.* House of Lords Select Committee on Communications. Retrieved from

www.publications.parliament.uk/pa/ld201617/ldselect/ldcomuni/130/130.pdf.

Hughes, S., & Vidano, L. (2015). *ISIS in America: From retweets to Raqqa*. Washington. Retrieved from https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/ISIS%20in%20America%20-%20Full%20Report.pdf.

Jones, L. M., Mitchell, K. J., & Finkelhor, D. (2012). Trends in youth internet victimization: Findings from three youth internet safety surveys 2000-2010. *The Journal of Adolescent Health, 50*(2), 179-86. doi: 10.1016/j.jadohealth.2011.09.015.

Juvonen, J., & Gross, E.F. (2008). Extending the school grounds? Bullying experiences in cyberspace. *Journal of School Health, 78*(9), 496-505. doi:10.1111/j.1746-1561.2008.00335.x.

Katz, A. (2014). *The cybersurvey for Suffolk.* Retrieved from http://dwn5wtkv5mp2x.cloudfront.net/downloads/Research_Highlights/UKCCIS_RH68_The_Cybersurvey_for_Suffolk.pdf.

Klettke, B., Hallford, D.J., & Mellor, D.J. (2014). Sexting prevalence and correlates: A systematic literature review. *Clinical Psychology Review, 34*(1), 44-53. doi:10.1016/j.cpr.2013.10.007.

Kowalski, R.M., Giumetti, G.W., Schroeder, A.N., & Lattanner, M.R. (2014). Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. *Psychological Bulletin, 140*(4), 1073-137.doi:10.1037/a0035618.

Lasher, S. & Baker, C. (2015) *Bullying: Evidence from the longitudinal study of young people in England 2, wave 2*. Research Brief. London: Department for Education.

Li, Q. (2010). Cyberbullying in high schools: A study of students' behaviors and beliefs about this new phenomenon. *Journal of Aggression, Maltreatment and Trauma, 19*(4), 372-92. doi:10.1080/10926771003788979.

Lilley, C., & Ball, R. (2013). *Younger children and social networking* sites. London: NSPCC. Retrieved from www.nspcc.org.uk/globalassets/documents/research-reports/younger-children-social-networking-sites-report.pdf.

Lilley, C., Ball, R., & Vernon, H. (2014). *The experience of 11-16 year olds on social networking sites.* London: NSPCC. Retrieved from www.nspcc.org.uk/globalassets/documents/research-reports/experiences-11-16-year-olds-social-networking-sites-report.pdf.

Livingstone, S. (2008). Taking risky opportunities in youthful content creation: Teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media & Society*, *10*(3), 393-411. Retrieved from http://eprints.lse.ac.uk/27072/.

Livingstone, S. (2013). Online risk, harm and vulnerability: Reflections on the evidence base for child internet safety policy. *ZER: Journal of Communication Studies, 18*(35), 13-28. Retrieved from http://eprints.lse.ac.uk/62278/.

Livingstone, S. (2014). Developing social media literacy: How children learn to interpret risky opportunities on social network sites. *Communications, 39*(3), 283-303. doi:10.1515/commun-2014-0113. Retrieved from http://eprints.lse.ac.uk/62129/.

Livingstone, S. & Helsper, E.J. (2007). Gradations in digital inclusion: Children, young people and the digital divide. *New Media & Society*, *9*(4), 671-96. doi:10.1177/1461444807080335.

Livingstone, S. & Helsper, E.J. (2008). Parental mediation and children's Internet use. *Journal of Broadcasting & Electronic media*, *52*(4), 581-99. Retrieved from http://eprints.lse.ac.uk/25723/.

Livingstone, S. & Mason, J. (2015). *Sexual rights and sexual risks among youth online: A review of existing knowledge regarding children and young people's developing sexuality in relation to new media environments*. Retrieved from http://eprints.lse.ac.uk/64567/.

Livingstone, S. & Palmer, T. (2012) *Identifying vulnerable children online and what strategies can help them.* London: UK Safer Internet Centre. Retrieved from http://eprints.lse.ac.uk/44222/.

Livingstone, S. & Smith, P. K. (2014). Annual research review: Harms experienced by child users of online and mobile technologies: The nature, prevalence and management of sexual and aggressive risks in the digital age. *Journal of Child Psychology and Psychiatry, 55*(6), 635-54. doi:10.1111/jcpp.12197

Livingstone, S., Haddon, L., Görzig, A., & Ólafsson, K. (2010). *Risks and safety on the internet: The UK report*. London: EU Kids Online, London School of Economics and Political Science. Retrieved from http://eprints.lse.ac.uk/33730/.

Livingstone, S., Görzig, A., & Ólafsson, K. (2011). *Disadvantaged children and online risk.* London: EU Kids Online, London School of Economics and Political Science. Retrieved from eprints.lse.ac.uk/39385/.

Livingstone, S., Haddon, L., Görzig, A., & Ólafsson, K. (2011). *EU Kids Online final report.* Retrieved from http://eprints.lse.ac.uk/39351/.

Livingstone, S., Kirwil, L., Ponte, C., & Staksrud, E. (2014b). In their own words: What bothers children online? *European Journal of Communication*, *29*(3), 271-88. Retrieved from http://eprints.lse.ac.uk/62093/ [For graphs, see the EU Kids Online report at http://eprints.lse.ac.uk/48357/]

Livingstone, S., Mascheroni, G., Ólafsson, K., & Haddon, L. (2014c) *Children's online risks and opportunities: Comparative findings from EU Kids Online and Net Children Go Mobile*. London: EU Kids Online, London School of Economics and Political Science. Retrieved from http://eprints.lse.ac.uk/60513/.

Livingstone, S., Ólafsson, K., O'Neill, B., & Donoso, V. (2012b). *Towards a better internet for children: Findings and recommendations from EU Kids Online to inform the CEO coalition*. London: EU Kids Online, London School of Economics and Political Science.

Livingstone, S., Davidson, J., Bryce, J., Millwood Hargrave, A., & Grove-Hills, J. (2012a). *Children's online activities, risks and safety: The UK evidence base.* London: UK Council for Child Internet Safety. Retrieved from http://eprints.lse.ac.uk/69571/.

Livingstone, S., Haddon, L., Vincent, J., Mascheroni, G., & Ólafsson, K. (2014a). *Net children go mobile: The UK report*. Retrieved from http://eprints.lse.ac.uk/57598/

Livingstone, S., Marsh, J., Plowman, L., Ottovordemgentschenfelde, S., & Fletcher-Watson, B. (2014d). *Young children (0-8) and digital technology: A qualitative exploratory study-*

national report-UK. Luxembourg: Joint Research Centre, European Commission. Retrieved from http://eprints.lse.ac.uk/60799/.

Livingstone, S., Mascheroni, G., Dreier, M., Chaudron, S., & Lagae, K. (2015). *How parents of young children manage digital devices at home: The role of income, education and parental style*. London: EU Kids Online, London School of Economics and Political Science. Retrieved from http://eprints.lse.ac.uk/63378/.

Livingstone, S., Olafsson, K., Helsper, E.J., Lupiáñez-Villanueva, F., Veltri, G.A., & Folkvord, F. (2017). Maximizing opportunities and minimizing risks for children online: The role of digital skills in emerging strategies of parental mediation. *Journal of Communication, 67*(1), 82-105. doi:10.1111/jcom.12277.

Lorenzo-Dus, N., Izura, C., & Pérez-Tattam, R. (2016). Understanding grooming discourse in computer-mediated environments. *Discourse, Context & Media, 12*, 40-50. doi:10.1016/j.dcm.2016.02.004.

Lupiáñez-Villanueva, F., Gaskell, G., Veltri, G., Theben, A., Folkford, F., Bonatti, L., et al. (2016). *Study on the impact of marketing through social media, online games and mobile applications on children's behaviour.* Brussels, Belgium: European Commission Directorate-General for Justice and Consumers. Retrieved from http://ec.europa.eu/consumers/consumer_evidence/behavioural_research/docs/final_report_impact_marketing_children_final_version_approved_en.pdf.

Macleod, M. (2012). *Digital parenting: An evaluation.* Vodafone. Retrieved from www.lgfl.net/downloads/online-safety/LGfL-OS-Research-Archive-2011-ParentZone-Digital-Parenting.pdf.

Martellozzo, E. (2012). *Online child sexual abuse: Grooming, policing and child protection in a multi-media world*. Abingdon: Routledge.

Martellozzo, E., Monaghan, A., Adler, J.R., Davidson, J., Leyva, R., & Horvath, M.A.H. (2016). *'…I wasn't sure it was normal to watch it…': A quantitative and qualitative examination of the impact of online pornography on the values, attitudes, beliefs and behaviours of children and young people.* London: Children's Commissioner and NSPCC. Retrieved from www.childrenscommissioner.gov.uk/sites/default/files/publications/MDX%20NSPCC%20OCC%20pornography%20report%20June%202016.pdf.

Mascheroni, G. & Ólafsson, K. (2014). *Net children go mobile: Risks and Opportunities* (2nd ed.). Milano: Educatt.

McDougall, J., & Livingstone, S., with Sefton-Green, J., & Fraser, P. (2014). *Media and information literacy policies in the UK*. Report for the COST (Transforming Audiences, Transforming Societies) initiative, Mapping Media Education Policies. Retrieved from http://eprints.lse.ac.uk/57103/.

McGuire, M., & Dowling, S. (2013). *Cyber crime: A review of the evidence*. Research Report 75 Chapter 1: Cyber-dependent crimes. Retrieved from www.gov.uk/government/uploads/system/uploads/attachment_data/file/246751/horr75-chap1.pdf.

Milnes, K., Turner-Moore, T., Gough, B., Denision, J., Gatere, L., Haslam, C., et al. (2015). *Sexual bullying in young people across European countries: Research report on the Addressing Sexual Bullying Across Europe (ASBAE) project.* Retrieved from

http://ec.europa.eu/justice/grants/results/daphne-toolkit/en/file/2924/download?token=LR_7bJf5.

Mitchell, K. J., Jones, L. M., Finkelhor, D., & Wolak, J. (2013). Understanding the decline in unwanted online sexual solicitations for US youth 2000-2010: Findings from three Youth Internet Safety Surveys. *Child Abuse & Neglect*, *37*(12), 122536. http://doi.org/10.1016/j.chiabu.2013.07.002.

Modecki, K.L., Minchin, J., Harbaugh, A.J., Guerra, N.G., & Runions, K.C. (2014). Bullying prevalence across contexts: A meta-analysis measuring cyber and traditional bullying. *Journal of Adolescent Health, 55*(5), 602-11.doi:10.1016/j.jadohealth.2014.06.007.

Mughal, S. (2016). *Radicalisation of young people on social media*. Retrieved from www.internetmatters.org/hub/expert-opinion/radicalisation-of-young-people-through-social-media/.

NCCU (National Cyber Crime Unit). (2017). *Intelligence assessment: Pathways into cyber crime*.

NCMEC (National Center for Missing & Exploited Children). (2015). Information taken from organisational website memorandums at www.missingkids.com/Exploitation.

NSPCC. (2016a). *What children are telling us about bullying: Childline bullying report 2015-16.* Retrieved from www.nspcc.org.uk/globalassets/documents/research-reports/what-children-are-telling-us-about-bullying-childline-bullying-report-2015-16.pdf.

NSPCC. (2016b). *'What should I do?' NSPCC helplines: Responding to children's and parents' concerns about sexual content online*. Retrieved from www.nspcc.org.uk/services-and-resources/research-and-resources/2016/what-should-i-do-helpline-report-online-abuse/.

NSPCC. (2016c). *Online child sexual abuse images: Doing more to tackle demand and supply*. Retrieved from www.nspcc.org.uk/globalassets/documents/research-reports/online-child-sexual-abuse-images.pdf.

NSPCC. (2016d) *Net Aware results report* (unpublished).

O'Neill, B. (2014). *First report on the implementation of the ICT principles*. Dublin: Dublin Institute of Technology. Retrieved from http://arrow.dit.ie/cgi/viewcontent.cgi?article=1056&context=cserart.

Ofcom. (2014a). *Children's online behaviour: Issues of risk and trust – Qualitative research findings*. Retrieved from www.ofcom.org.uk/__data/assets/pdf_file/0028/95068/Childrens-online-behaviour-issues-of-risk-and-trust.pdf.

Ofcom. (2014b). *Ofcom report on internet safety measures – Internet service providers: Network level filtering measure*. Retrieved from www.ofcom.org.uk/__data/assets/pdf_file/0019/27172/Internet-safety-measures-second-report.pdf.

Ofcom. (2016a). *Children and parents: Media use and attitudes report.* Retrieved from www.ofcom.org.uk/__data/assets/pdf_file/0034/93976/Children-Parents-Media-Use-Attitudes-Report-2016.pdf.

Ofcom. (2016b). *Children's media lives – Year 2 findings*. Retrieved from www.ofcom.org.uk/__data/assets/pdf_file/0021/80715/children_media_lives_year2.pdf.

Opinion Leader (2013). *Cybersafe: Research to support a safer internet campaign*. Retrieved from www.internetmatters.org/wp-content/uploads/2015/12/Cybersafe-20-Sept-2013-Opinion-Leader-FINAL-VERSION-1.pdf.

Palladino, B. E., Nocentini, A., & Menesini, E. (2016). Evidence-based intervention against bullying and cyberbullying: Evaluation of the NoTrap! Program in two independent trials. *Aggressive Behavior*, *42*(2), 194-206. doi:10.1002/ab.21636.

Palmer, T. (2015). *Digital dangers: The impact of technology on the sexual abuse and exploitation of children and young people*. Ilford: Barnado's. Retrieved from www.barnardos.org.uk/digital_dangers_report.pdf.

Parker, I. (2014). *Young people, sex and relationships the new norms*. London: Institute for Public Policy Research (IPPR). Retrieved from http://www.ippr.org/files/publications/pdf/young-people-sex-relationships_Aug2014.pdf?noredirect=1.

Peter, J., & Valkenburg, P. M. (2016). Adolescents and pornography: A review of 20 years of research. *The Journal of Sex Research, 53*(4–5), 509-31. doi:10.1080/00224499.2016.1143441

Phippen, A. (2009). *Sharing personal images and files among young people*. Exeter: South West Grid for Learning. Retrieved from http://webfronter.com/surreymle/devonesafety/other/Sexting%20report%20-%20andy%20phippen.pdf

Polak, M. (2007). 'I think we must be normal… There are too many of us for this to be abnormal!!!' Girls creating identity and forming community in Pro-Ana/Mia websites. In S. Weber & S. Dixon (Eds.) *Growing up online: Young people and digital technologies* (pp. 83-96). New York: Palgrave Macmillan.

Priebe, G., Mitchell, K. J., & Finkelhor, D. (2013). To tell or not to tell? Youth's responses to unwanted Internet experiences. *Cyberpsychology*, *7*(1). doi:10.5817/CP2013-1-6.

Przybylski, A.K. & Nash, V. (2017). Internet filtering technology and aversive online experiences in adolescents. *The Journal of Pediatrics*, In press. doi:10.1016/j.jpeds.2017.01.063.

Przybylski, A.K., Mishkin, A., Shotbolt, V., & Linington, S. (2014). *A shared responsibility: Building children's online resilience*. London: Virgin Media and Parent Zone.

Quayle, E., & Newman, E. (2016). An exploratory study of public reports to investigate patterns and themes of requests for sexual images of minors online. *Crime Science, 5*(2). doi:10.1186/s40163-016-0050-0

Quayle, E., Goren Svedin, C., & Jonsson, L. (2017). Children in identified sexual images – Who are they? Self and non-self-taken images. In the International Child Sexual Exploitation image database (ICSE DB) 2006-15. Child Abuse Review (accepted January 2017).

Quayle, E., Jonsson, L., & Lööf, L. (2012). *Online behaviour related to child sexual abuse. Interviews with affected young people: ROBERT – Risktaking Online Behaviour, Empowerment through Research and Training*. European Union & Council of the Baltic Sea State.

Ringrose, J., Gill, R., Livingstone, S., & Harvey, L. (2012). *A qualitative study of children, young*

people and 'sexting'. London: NSPCC. Retrieved from http://eprints.lse.ac.uk/44216/.

Schultze-Krumbholz, A., Schultze, M., Zagorscak, P., Wölfer, R., & Scheithauer, H. (2016). Feeling cybervictims' pain: The effect of empathy training on cyberbullying. *Aggressive Behavior*, *42*(2), 147-56. doi:10.1002/ab.21613.

Seto, M. (2016). Research on online sexual offending: What have we learned and where are we going? *Journal of Sexual Aggression*, *23*(1), 104-6. doi:10.1080/13552600.2016.1251021.

Shipton, L. (2011). *Improving e-safety in primary schools: A guidance document*. Sheffield: Centre for Education and Inclusion Research, Sheffield Hallam University. Retrieved from www4.shu.ac.uk/_assets/pdf/ceir-improving-e-safety-primary-schools-guidance.pdf.

Smahel, D. & Wright, M. F. (Eds.) (2014). *Meaning of online problematic situations for children. Results of qualitative cross-cultural investigation in nine European countries*. London: EU Kids Online, London School of Economics and Political Science. Retrieved from http://eprints.lse.ac.uk/56972/.

Stanley, N., Barter, C., Wood, M., Aghtaie, N., Larkins, C. Lanau, A., et al. (2016). Pornography, sexual coercion and abuse and sexting in young people's intimate relationships: A European study. *Journal of Interpersonal Violence*. doi:10.1177/0886260516633204.

STIR (n.d.). *Connecting online and offline contexts and risks*. Retrieved from http://stiritup.eu/wp-content/uploads/2015/06/STIR-Exec-Summary-English.pdf.

Tokunaga, R.S. (2010). Following you home from school: A critical review and synthesis of research on cyberbullying and victimization. *Computers in Human Behaviour, 26*(3), 277-87. doi:10.1016/j.chb.2009.11.014.

UK Safer Internet Centre (2016a). *Creating a better internet for all: Young people's experiences of online empowerment + online hate*. Retrieved from http://childnetsic.s3.amazonaws.com/ufiles/SID2016/Creating%20a%20Better%20Internet%20for%20All.pdf.

UK Safer Internet Centre (2016b). *Safer Internet Day 2016: Impact report.* Retrieved from http://www.saferinternet.org.uk/sites/default/files/Safer%20Internet%20Day%202016/Safer-Internet-Day-2016-impact-report.pdf.

UK Safer Internet Centre (2017). *Power of image: A report into the influence of images and videos in young people's digital lives*. Retrieved from www.saferinternet.org.uk/safer-internet-day/2017/power-of-image-report.

UKCCIS (UK Council for Child Internet Safety) (2016). *Sexting in schools and colleges: Responding to incidents and safeguarding young people.* Retrieved from www.gov.uk/government/uploads/system/uploads/attachment_data/file/551575/6.2439_KG_NCA_Sexting_in_Schools_WEB__1_.PDF.

van Ouytsel, J., Van Gool, E., Ponnet, K., & Walrave, M. (2014). Brief report: The association between adolescents' characteristics and engagement in sexting. *Journal of Adolescence*, *37*, 1387-91. doi:10.1016/j.adolescence.2014.10.004.

van Ouytsel, J., Walrave, M., Ponnet, K., Heirman, W. (2015). The association between adolescent sexting, psychosocial difficulties, and risk behavior: Integrative review. *The Journal of School Nursing, 31*(1), 54-69. doi:10.1177/1059840514541964.

van Royen, K., Vandebosch, H., & Poels, K. (2015). Severe sexual harassment on social networking sites: Belgian adolescents' views. *Journal of Children and Media*, *9*(4), 472-91. doi:10.1080/17482798.2015.1089301.

Vandoninck, S., d'Haenens, L., & Smahel, D. (2014). *Preventive measures – How youngsters avoid online risks*. London: EU Kids Online, London School of Economics and Political Science. Retrieved from http://eukidsonline.metu.edu.tr/file/Preventivemeasures.pdf.

von Behr, I., Reding, A., Edwards, C., & Gribbon, L. (2013). *Radicalisation in the digital era: The use of the internet in 15 cases of terrorism and extremism*. Cambridge. Retrieved from www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf.

von Knop, K. (2007). Countering web-based Islamist narratives: conceptualising an information war and a counter-propaganda campaign. In B. Ganor, K. von Knop, & C. Duarte (Eds.) *Hypermedia seduction for terrorist recruiting* (pp. 245-66). Amsterdam: IOS Press.

Watters, P.A. (2014). *A systematic approach to measuring advertising transparency online: An Australian case study*. Proceedings of the Second Australasian Web Conference – Volume 155, 59-67. Retrieved from http://dl.acm.org/citation.cfm?id=2667708.

Webster, S., Davidson, J., & Bifulco, A. (2014). *Online offending behaviour and child victimisation: New findings and policy*. Basingstoke: Palgrave Macmillan.

Webster, S., Davidson, J., Bifulco, A., Gottschalk, P., Caretti, V., Pham, T., et al. (2012). *European Online Grooming Project final report*. Retrieved from www.cats-rp.org.uk/pdf files/EUGP_Final_Ex_Summary130412.pdf.

Whittle, H. C., Hamilton-Giachritsis, C. E., & Beech, A. R. (2014). 'Under his spell': Victims' perspectives of being groomed online. *Social Sciences, 3*(3), 404-26.

WISEKIDS (2014). *Generation 2000: The internet and digital media habits and digital literacy of year 9 pupils (13 and 14 year olds in Wales*. Retrieved from http://wisekids.org.uk/wk/wp-content/uploads/2014/12/EnglishFinal.pdf.

Wood, M., Barter, C., Stanley, N., Aghtaie, N., & Larkins, C. (2015). Images across Europe: The sending and receiving of sexual images and associations with interpersonal violence in young people's relationships. *Children & Youth Services Review, 59*, 149-60. doi:10.1016/j.childyouth.2015.11.005

Xu, Z., Hu, Q., & Zhang, C. (2013). Why computer talents become computer hackers. *Communications of the ACM, 56*(4). doi:10.1145/2436256.2436272.

Ybarra, M. L., & Mitchell, K. J. (2005). Exposure to internet pornography among children and adolescents: A national survey. *CyberPsychology & Behavior*, *8*(5), 473-86. doi:10.1089/cpb.2005.8.473

Youth Justice Board. (2012a). *Preventing religious radicalisation and violent extremism: A systematic review of the research evidence.* Retrieved from www.gov.uk/government/uploads/system/uploads/attachment_data/file/396030/preventing-violent-extremism-systematic-review.pdf.

Youth Justice Board (2012b). *Process evaluation of preventing violent extremism programmes for young people*. Retrieved from http://dera.ioe.ac.uk/16233/1/preventing-violent-extremism-

process-evaluation.pdf.

Zych, I., Ortega-Ruiz, R., & Del Ray, R. (2015). Systematic review of theoretical studies on bullying and cyberbullying: Facts, knowledge, prevention, and intervention. *Aggression and Violent Behavior, 23*(July-August), 1-21. doi:10.1016/j.avb.2015.10.001