HOUSES OF PARLIAMENT
PARLIAMENTARY OFFICE OF SCIENCE & TECHNOLOGY

POSTNOTE

Number 608 July 2019

Online Safety Education

Online technology is now an integral part of children's lives. This POSTnote summarises the available evidence on how the internet impacts on outcomes. It gives an overview of current online safety education and resources available to parents and teachers, and examines the role of technology in improving online safety.

Overview

- The internet presents young people with opportunities (such as developing skills) and risks (such as running into harmful content).
- There is limited evidence on impacts; certain online activities may be associated with positive outcomes (such as improved relationships) or negative outcomes (such as lowered self-esteem).
- In England, new mandatory relationships education, relationships and sex education, and health education will teach some aspects of online safety from 2020.
- Some teachers, parents and police report a lack of knowledge around online safety.
- Technology can help mitigate some online risks. The UK Government has proposed new regulations for internet companies.

Background

A 2018 Ofcom survey of 1304 parents of children aged 5–15 years who go online in the UK found that many were concerned about their children's activity on the internet.[1] In 2017, the Children's Commissioner for England identified shortcomings in online safety education and a number of stakeholders, including the Commons Digital, Culture, Media and Sport (DCMS) Committee, have recommended action to increase 'digital literacy' in the UK.[2–6]

Several government bodies are involved in children's online safety (Box 1). In 2019, the Home Office and DCMS's Online Harms White Paper proposed a UK-wide online media literacy strategy and a new duty of care for internet companies, overseen by an independent regulator.[7] Online safety will be taught in all primary and secondary schools in England from September 2020 as part of changes to the curriculum.[8] As education is a devolved matter, education-related content in this note will focus mainly on England.

This POSTnote provides an overview of how children use the internet, and what opportunities and risks this presents; current online safety education in schools and elsewhere, and how this will be affected by curriculum changes; examples of online safety resources available to parents, teachers and other professionals; and the role of technology (such as content filtering) in enhancing online safety.

Trends in internet use

Ofcom reports that 92% of children aged 5–15 years in the UK now use the internet.[1] The frequency and duration of children's internet use has increased over the last decade: the average amount of time spent on the internet per week by children aged 5–15 rose from 9 hours in 2009 to 15 hours in 2018.[1] Children aged 7–16 years report that they go online to watch videos (59%), listen to music (56%), play games (54%), complete homework (47%), message friends or family (47%), and for social networking (40%).[9] Technology such as touch screens or 'smart' (internet-connected) toys also offer opportunities for pre-literate children: 52% of children aged 3–4 years use the internet for activities such as watching videos and playing games.[1]

Age is a major factor in internet use, with children increasingly likely to go online as they get older.[1] There are also changes in how and where children access the internet as they age. Children under the age of 12 years primarily access the internet using a tablet, whereas those aged 12–15 tend to use a mobile phone.[1] Although the main location for online activity for all age groups is in the home, time spent online in private spaces or outside the home increases with age.[1,10,11] Looked after children may face additional barriers to accessing the internet, with evidence suggesting that internet access in residential children's homes is inconsistent.[12]

Opportunities and risks

Children and parents have differing attitudes towards the internet.[13] A survey of 1512 adolescents aged 13–18 years found that 72% agreed that the internet can be used to bring young people closer together.[14] However, young people also have concerns, including about pornographic or violent content, inappropriate contact and cyber-bullying.[15] Although many parents feel that their children benefit from digital engagement, research suggests that parental concern about online risks is rising.[1] The 2018 Ofcom survey found that the primary concern among parents (expressed by 50% of respondents) was companies collecting data on their children's online activity. Concerns also included reputational damage (42%), giving out personal details to inappropriate people (41%) and pressure to spend money online (41%), among others.[1]

Some stakeholders say that classifying particular online activities or services as presenting either 'opportunities' or 'risks' can be difficult and overly simplistic, as many offer both.[15] For example, contacting new people online is sometimes referred to as a 'risky opportunity' because it may allow children to make friends, while also potentially exposing them to inappropriate contact.[15] The academic literature about the impacts of online opportunities and risks on outcomes (such as educational attainment or mental well-being) is limited and mainly identifies associations without identifying causation.[15,16] Outcomes are also influenced by many other competing factors, making it difficult to isolate the effect of online opportunities/risks.[17] This section summarises the opportunities and risks faced by children online and the available evidence on outcomes.

Online opportunities

Children aged 12–15 years who go online use the internet for a wide range of activities, such as socialising (70% have a social media account), help with schoolwork (64% have used BBC resources for school work), undertaking creative activities (70%) or engaging civically (8% sign petitions, 12% support causes or organisations online).[1] There is evidence that having internet access improves educational outcomes, such as improved GCSE results.[18,19] Although outcomes can be hard to measure, children and young people report positive effects of online opportunities.[20] For example, a survey of young people aged 11–25 years found that 62% believe that social media has a positive impact on their relationships with friends.[21] Children isolated due to mental ill health report finding support from peers online.[21]

Risks faced by children online

Types of risks

Online risks faced by children are commonly grouped into four categories:[22,23]

- **Content.** This includes age inappropriate material, such as pornography and violent content, and 'fake news'.
- **Contact.** The risk of being radicalised or contacted by people who seek to victimise them.
- **Conduct.** Risks that involve a child as a perpetrator, or behaviour such as oversharing personal information, cyber-bullying, or creating and sharing sexual images.
- **Commercial.** The risk of being exposed to advertising, hidden costs in games, online gambling or data collection.

Box 1: The roles of governmental and regulatory bodies

- **Government departments**: The Department for Education sets requirements on online safety education and safeguarding in schools in England; DCMS is responsible for online safety across all age groups; and the Home Office is responsible for tackling cybercrime and online child sexual abuse and exploitation, primarily through the non-ministerial department, the National Crime Agency (NCA).[24–27] The NCA operates the Child Exploitation and Online Protection (CEOP) Command, which works to protect children through law enforcement, safeguarding and education.[28,29]
- **Regulators**: Ofsted is responsible for inspecting maintained schools and academies, and some independent schools in England.[30] Ofcom is the regulator for communications services. It has a duty to promote and carry out research into media literacy.[31,32] The British Board of Film Classification is the regulator for age-verification under the Digital Economy Act 2017.[33] The Information Commissioner is tasked with upholding information rights and data privacy.[34] She has enforcement powers and aims to educate the public about data protection.[35]
- **Other public bodies**: The Children's Commissioner for England has a legal mandate to promote and protect the rights of children.[36]
- **Voluntary sector**: The UK Council for Internet Safety is a collaborative forum formed of government, technology companies, and third sector organisations. It reviews evidence, coordinates cross-sector projects, and supports good practice.[37]

The extent to which children are subject to these risks depends on various demographic factors.[38] Girls are disproportionately subject to online sexual harassment and re-sharing of sexual images: a 2015 survey of children aged 14–16 years found that of those who had sent a sexual image to a partner, 42% of girls reported the image being shared by their partner compared with 13% of boys.[39] Vulnerable young people (including children with disabilities, in care, experiencing family difficulties or from marginalised groups) are more likely to encounter risks online and find them harmful.[40] For example, young carers are 20% more likely to be cyber-bullied.[41] As children grow older, they usually engage in a broader range of activities online and face more risks in general.[10] However, data suggest that their digital skills also improve and so they may be better equipped to deal with risks.[38]

Evidence on outcomes

Evidence on outcomes focuses on associations between risks and outcomes because exposing children to risks to explore causation, or asking them about certain experiences, would be unethical.[42] Some of the risks that have been studied are as follows.

- **Exposure to pornography** is correlated with attitudes such as unrealistic perceptions of sex and may be correlated with aggressive sexual behaviour.[15,43]
- **Cyber-bullying** is linked with similar problems to bullying offline, such as depression and lowered self-esteem.[44,45]
- **Online child sexual exploitation and abuse** may involve coercing or manipulating a child to engage in sexual activity online, such as video streaming, or to meet offline.[46] The evidence suggests that impacts are similar to those from offline abuse, which include post-traumatic stress disorder and social difficulties.[47,48]

- **Sexting** (sharing of sexual images) has mainly been studied through surveys. One survey found that 58% of young people in relationships viewed sexting as a positive activity.[39] However, re-sharing of sexts is associated with severe distress and reputational damage.[15,49] There are also legal risks, as the production, possession or sharing of sexual images of under-18s is illegal.[50,51]

Many stakeholders, including parents, teachers and children, have expressed concerns about the potential negative impacts of social media, self-harm and pro-eating disorder content on children's mental health.[21,52–54] Despite evidence of the positive impacts of social media, its use has been linked to anxiety and decreased well-being.[55–57] Many groups have identified a lack of evidence in this area and there have been calls for social media companies to share anonymised data for research.[20] The government's proposed regulator for technology (tech) companies (Box 2) will encourage companies to share anonymised data.[7]

Equipping children for life online

There has been increasing interest in fostering 'digital resilience' in children rather than trying to shield them from all risks online.[3,58] The UK Council for Internet Safety (UKCIS) defines digital resilience as the ability to identify online risks and to deal with and learn from difficult experiences online.[59] Evidence suggests that both positive and negative experiences online can contribute to a child's digital resilience.[58,60] Many agree that education plays an important role,[2,3] however, there is a lack of evidence on effective practice in this area.[61] NCA-CEOP commissioned the PSHE Association – a national body for Personal, Social, Health and Economic (PSHE) education professionals – to produce a set of principles for effective preventive education informed by schools-based programmes in other areas (Box 3).[61] Many stakeholders agree that tech companies, including online platforms, need to do more to create safe online environments for children, with many supporting the government's proposed statutory duty of care for tech companies (Box 2).[23,62–64]

Current curriculum in England

Education policy is devolved so online safety teaching differs across the UK (Box 4). This section considers online safety teaching in England. Statutory guidance requires all schools in England to teach online safety as part of a 'broad and balanced curriculum'.[65]

- **The computing curriculum** is compulsory in local authority schools from year 1 until age 16.[66] The curriculum includes safe, secure and responsible use of technology, and how to deal with concerns about online risks.[67] Other schools may also optionally teach about online safety in computing lessons.
- **PSHE** is currently only compulsory in independent schools. However some form of PSHE is taught at 93% of all schools in England.[68] About 80% of schools deliver some online safety as part of PSHE lessons.[69] The PSHE Association has produced a programme of study that the Department for Education advises schools to use.[70,71]
- **Assemblies and external trainers** are also used to deliver online safety education.[69] Although these events can provide significant benefits, UKCIS advises that over-reliance on these approaches or treatment of online safety education as a "one-off" can be counterproductive (Box 3).[72] It may also disadvantage vulnerable children due to their school attendance generally being lower.[73]

Box 2: Regulation of tech companies

- **Online Harms White Paper.** Tech companies have implemented measures aiming to reduce harm to their users, such as moderation and safety policies.[74] In 2019, the UK government published the Online Harms White Paper, which stated that these measures "have not gone far or fast enough, or been consistent enough".[7] The White Paper outlined proposals to establish a duty of care for internet companies that will make clear companies' responsibilities to keep users safe.[7] This will be enforced by an independent regulator whose powers will include levying fines and may include holding senior management individually liable.[7] Consultation on the White Paper closed on 1st July 2019.
- **Age-Appropriate Design Code.** Concerns have been raised that tech companies prioritise commercial interests over users' (particularly children's) well-being.[75] To combat this, the Data Protection Act 2018 requires the Information Commissioner to produce an 'age-appropriate design code', to set design standards for services likely to be used by children.[76] A draft code has been published and has recently undergone consultation. It states that the best interests of the child should be a primary design consideration and sets standards on 16 aspects, including the collection and use of children's data, profiling and transparency.[77]

Planned changes to the curriculum in England

Aspects of PSHE will become compulsory in all schools in England: Relationships education will become compulsory in all primary schools, and relationships and sex education (RSE) compulsory in all secondary schools from September 2020 (POSTnote 576).[78] Health education will also become compulsory for all ages in state-funded schools from 2020. The government has published guidance for these subjects, and some schools will teach the new content from 2019.[8] At primary level, guidelines state relationships education should cover topics such as how to recognise risks and get support, respectful online relationships, and data and privacy.[8] At secondary level, RSE will include pupils' rights, responsibilities and opportunities online, how the internet can promote an unrealistic image of relationships or sex, and the risks of sharing sexual images.[8] Health education will include the impacts of online activities on children's wellbeing.[8] The guidance notes resources such as UKCIS's 'Education for a Connected World', which describes the skills that children should have the opportunity to develop at different stages.[8,79] The guidance relating to online safety in these new subjects has been broadly welcomed by stakeholders.[80] The government plans to produce information on how schools can teach online safety across the curriculum.[81]

Beyond the curriculum

There is a role for schools, parents and others outside formal education (such as professionals working with children in social care or medicine) to promote online safety.

Box 3: Principles associated with effective online safety teaching
Noting the lack of evidence around effective practice in online safety education, NCA-CEOP commissioned the PSHE Association to review evidence from school-based preventive education in areas, such as drug and alcohol use, in order to develop principles to inform preventive education in general.[61] The principles include: providing high-quality training and support for teachers; starting teaching early enough to have an impact on future behaviour; creating a programme that is delivered regularly and progresses logically; tailoring content for the needs of students; and taking a 'whole-school' approach, where online safety education is embedded into wider school policies or other curriculum subjects.

Schools

A 'whole-school' approach to online safety is recognised as good practice (Box 3).[82] However, analysis of 14,000 schools across the UK found that about 50% of schools have no engagement with the community on online safety, and about 40% do not involve pupils in developing their online safety strategy.[83] The same data found that 43% of schools have no staff training for online safety, and 50% have no online safety training for governors.[83]

Other professionals working with children

Front line staff, such as police or social workers, play an important role in identifying children who are at risk online and intervening.[84,85] For example, 69% of police officers report dealing with online child sexual abuse at least annually.[84] A 2016 project by the Better Policing Collaborative reported that professionals working with children felt they have not had sufficient training to respond effectively to complaints of online harm, and identified a lack of coordination between organisations.[85] Resources are available for professionals working with children, such as Keeping Children Safe Online, an e-learning course developed by children's charity the NSPCC and NCA-CEOP.[86,87] NCA-CEOP also run one-day Ambassador courses for professionals working with children.[88] There has been no robust analysis of the effect these programmes have on outcomes such as behaviour.

Parental involvement

Communication between parents and children is a key factor in children's development of digital skills.[58] 81% of parents of children aged 5–15 said that they have talked to their children about online safety; 40% do so at least every few weeks.[1] However, parents may lack the understanding to help their children with online safety.[3] For example, 32% of parents of children aged 5–15 who use Facebook knew that the minimum age required to create a profile is 13.[1] Describing children as 'digital natives' (very familiar with technology), may make parents less confident talking to children, and children less likely to ask for help. This term can also be misleading as children's actual digital skills are often shallow.[85] Resources are available to inform or train parents, such as materials from Internet Matters, Childnet, Parent Zone, NSPCC, Thinkuknow or the UK Safer Internet Centre, but there is little robust analysis of how they affect outcomes such as behaviour.[15,89–95] NCA-CEOP will evaluate its Thinkuknow programme in 2019–20 to measure its impact on children's behaviour and knowledge.

Box 4: Online safety education in the devolved nations

- **Wales:** Local authority-maintained schools are required to teach online safety within Information and Communication Technology (ICT) and encouraged to do so within Personal and Social Education.[96–98] The Welsh Government will introduce a new curriculum for primary and secondary pupils between 2022 and 2026 and is currently taking feedback on a draft version. As part of this, digital competence will become one of three cross-curricular responsibilities for schools.[99,100]
- **Scotland:** With very few exceptions, the school curriculum in Scotland is non-statutory. However, the national Curriculum for Excellence includes digital literacy, which covers internet safety and cyber resilience.[101,102]
- **Northern Ireland**: Online safety is taught in ICT in primary and secondary schools.[103,104] Aspects of online safety may also be taught in non-statutory RSE in secondary schools.

Peer-to-peer programmes

Peer-to-peer programmes have been suggested as an effective way to teach about controversial topics, as children may feel more comfortable talking with people their own age about these issues.[106] The Childnet Digital Leaders Programme, used by 720 schools, aims to equip young people to mentor peers and advocate for online safety.[107] There is no robust analysis of how it affects outcomes.

The role of technology

Safety technologies that aim to protect children online include content filtering and age-verification. The proposed new online regulator (Box 2) is planned to encourage development and adoption of safety technologies.[7]

- **Filtering** blocks websites that contain inappropriate content. Filters can be applied by an internet service provider (ISP) to block certain websites for devices connected to a network, or by software on a device. The four largest ISPs all offer their customers the option to apply a filter to their home internet network.[108] The 2018 Ofcom survey found that 34% of parents use ISP content filters at home.[1] Schools in England and Wales have an obligation to ensure appropriate filtering is in place.[65,109] Some evidence suggests that filters are not effective at shielding adolescents aged 12–15 from aversive online experiences.[110] Research has also found that, while filters can directly protect children from harm, their use may undermine a child's online resilience,[58] and some say that internet restrictions may infringe on children's rights.[111–113]
- **Age-verification** refers to technologies that attempt to establish the age of a user. Under the Digital Economy Act 2017, pornography websites will be required to use 'robust' age-verification to ensure their users are 18 or over; this will be enforced by the British Board of Film Classification.[114,115] This policy was due to come into force in July 2019, but the government recently announced a delay of around 6 months.[116] Some stakeholders, including the Open Rights Group, have raised privacy concerns about the handling of age verification data.[117] Several companies have developed age verification systems that porn websites may use. These give users the option to provide credit card details or identity documents, or buy a pass in person after showing identification.[118]

POST is an office of both Houses of Parliament, charged with providing independent and balanced analysis of policy issues that have a basis in science and technology. POST is grateful to Dugald Hepburn for researching this briefing, to the STFC for funding his parliamentary fellowship, and to all contributors and reviewers. For further information on this subject, please contact the co-author, Dr Lorna Christie.

Endnotes

1. Ofcom (2018). *Children and Parents: Media Use and Attitudes Report 2018.*
2. House of Lords Select Committee on Communications (2017). *Growing up with the internet.*
3. Children's Commissioner (2017). *Growing Up Digital.*
4. House of Lords Select Committee on Political Polling and Digital Media (2018). *The politics of polling.*
5. Department for Digital, Culture, Media and Sport Committee (2019). *Disinformation and 'fake news'.*
6. 5Rights Foundation [online].The Right to Digital Literacy. Accessed 25/07/19.
7. HM Government (2019). *Online Harms White Paper.*
8. Department for Education (2019). *Relationships Education, Relationships and Sex Education (RSE) and Health Education: Statutory guidance for governing bodies, proprietors, head teachers, principals, senior leadership teams, teachers.*
9. Childwise (2017). *Monitor report 2017: Children's media use and purchasing*.
10. Livingstone, S. *et al.* (2014). *Net children go mobile: the UK report: a comparative report with findings from the UK 2010 survey by EU Kids Online.*
11. Livingstone, S. *et al.* (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.*
12. Children's Commissioner (2017). *Growing Up Digital In Care.*
13. Vandoninck, S. *et al.* (2014). *Preventive measures: how youngsters avoid online risks.* EU Kids Online.
14. UK Safer Internet Centre (2016). *Creating a Better Internet for All.*
15. Livingstone, S. *et al.* (2017). *Children's online activities, risks and safety: a literature review by the UKCCIS evidence group.* UKCCIS.
16. Slavtcheva-Petkova, V. *et al.* (2015). Evidence on the extent of harms experienced by children as a result of online risks: implications for policy and research. *Inf. Commun. Soc.*, Vol 18, 48–62.
17. Kardefelt-Winther, D. (2017). How Does the Time Children Spend Using Digital Technology Impact their Mental Well-being, Social Relationships and Physical Activity? *Innocenti Discuss. Pap.*, Vol no. 2017-02,
18. Joseph Rowntree Foundation (2010). *Poorer children's educational attainment: how important are attitudes and behaviour?*
19. Department for Education (2011). *Evaluation of the home access programme: final report.*
20. House of Commons Science and Technology Committee (2019). *Impact of social media and screen-use on young people's health.*
21. The Children's Society *et al.* (2018). *Safety Net: Cyberbullying's impact on young people's mental health.*
22. Safer Internet Centre [online]. What are the issues? Accessed 25/07/19.
23. 5Rights Foundation (2019). *Towards an Internet Safety Strategy.*
24. GOV.UK [online]. Department for Education single departmental plan. Accessed 25/07/19.
25. GOV.UK [online]. Home Office single departmental plan. Accessed 25/07/19.
26. GOV.UK [online]. Department for Digital, Culture, Media and Sport single departmental plan. Accessed 25/07/19.
27. National Crime Agency [online]. What we investigate. Accessed 25/07/19.
28. Child Exploitation and Online Protection command [online]. Terms and Conditions. Accessed 25/07/19.
29. Thinkuknow [online]. Welcome to Thinkuknow. Accessed 25/07/19.
30. GOV.UK [online]. Ofsted About us. Accessed 25/07/19.
31. Ofcom [online]. What is Ofcom? Accessed 25/07/19.
32. Ofcom [online]. About media literacy. Accessed 25/07/19.
33. BBFC [online]. Age-verification under the Digital Economy Act 2017. Accessed 25/07/19.
34. Information Commissioner's Office [online]. What we do. Accessed 25/07/19.
35. Information Commissioner's Office [online]. Your data matters. Accessed 25/07/19.
36. Children's Commissioner [online]. Children's Commissioner for England. Accessed 25/07/19.
37. GOV.UK [online]. UKCIS About us. Accessed 25/07/19.
38. Livingstone, S. *et al.* (2012). *Children, risk and safety on the internet: research and policy challenges in comparative perspective*. Policy Press.
39. Wood, M. *et al.* (2015). Images across Europe: The sending and receiving of sexual images and associations with interpersonal violence in young people's relationships. *Child. Youth Serv. Rev.*, Vol 59, 149–160.
40. Livingstone, S. *et al.* (2012). *Identifying vulnerable children online and what strategies can help them.* UKCCIS.
41. Katz, A. (2016). *The Suffolk Cybersurvey 2016.* Youthworks Consulting.
42. Livingstone, S. (2013). Online risk, harm and vulnerability: reflections on the evidence base for child Internet safety policy. *ZER J. Commun. Stud.*, Vol 18, 13–28.
43. Horvath, M. A. H. *et al.* (2013). *Basically... porn is everywhere: a rapid evidence assessment on the effects that access and exposure to pornography has on children and young people.*
44. Kowalski, R. M. *et al.* (2014). Bullying in the digital age: a critical review and meta-analysis of cyberbullying research among youth. *Psychol. Bull.*, Vol 140, 1073–1137.
45. Zych, I. *et al.* (2015). Systematic review of theoretical studies on bullying and cyberbullying: Facts, knowledge, prevention, and intervention. *Aggress. Violent Behav.*, Vol 23, 1–21.
46. Department for Education (2017). *Child sexual exploitation.*
47. Whittle, H. C. *et al.* (2013). Victims' Voices: The Impact of Online Grooming and Sexual Abuse. *Univers. J. Psychol.*, 13.
48. Hamilton-Giachritsis, C. *et al.* (2017). *"Everyone deserves to be happy and safe": a mixed methods study exploring how online and offline child sexual abuse impact young people and how professionals respond to it.* NSPCC.
49. NSPCC (2016). *"What should I do?" NSPCC helplines: responding to children's and parents' concerns about sexual content online.*
50. College of Policing (2016). *Police action in response to youth produced sexual imagery ('Sexting').*
51. UKCCIS (2017). *Sexting in schools and colleges: Responding to incidents and safeguarding young people.*
52. Crawford, A. (2019). Instagram eating disorder content 'out of control'. *BBC*.
53. Udorie, J. E. (2015). Social media is harming the mental health of teenagers. The state has to act. *The Guardian*.
54. Malik, J. (2019). 'Unacceptable' self-harm still on Instagram. *BBC*.
55. McCord, B. *et al.* (2014). Facebook: Social uses and anxiety. *Comput. Hum. Behav.*, Vol 34, 23–27.
56. Kross, E. *et al.* (2013). Facebook Use Predicts Declines in Subjective Well-Being in Young Adults. *PLOS ONE*, Vol 8, e69841.
57. Steinfield, C. *et al.* (2008). Social capital, self-esteem, and use of online social network sites: A longitudinal analysis. *J. Appl. Dev. Psychol.*, Vol 29, 434–445.
58. Przybylski, A. *et al.* (2014). *A Shared Responsibility: Building Children's Online Resilience.*
59. Bush, M. *et al.* (2016). *Resilience for the Digital World.* YoungMinds.
60. Rosen, R. (2017). *Ordinary magic for the digital age: understanding children's digital resilience.* Parent Zone.
61. PSHE Association (2016). *Key principles of effective prevention education.*
62. NSPCC (2019). *Taming the wild west web: regulate social networks.*
63. Children's Commissioner (2018). *Who knows what about me?*
64. Barnardo's (2019). *Barnardo's backs calls for social media companies to have a 'duty of care' for children.*
65. Department for Education (2018). *Keeping children safe in education.*
66. Department for Education (2014). *The national curriculum in England.*
67. Department for Education (2013). *National curriculum in England: computing programmes of study.*

68. Smith, R. *et al.* (2018). *Teacher Voice Omnibus Survey.* Department for Education.
69. UK Safer Internet Centre (2015). *Ofsted reveals new 'Online Safety in Schools' survey.*
70. PSHE Association (2017). *PSHE Education Programme of Study (Key stage 1-5).*
71. Department for Education (2013). *Personal, social, health and economic (PSHE) education.*
72. UK Council on Child Internet Safety (2018). *Using External Visitors to Support Online Safety Education.*
73. Katz, A. *et al.* (2019). *Vulnerable Children in a Digital World.* Internet Matters.
74. Facebook [online]. Community Standards. Accessed 25/07/19.
75. Kidron, B. *et al.* (2018). *Disrupted Childhood: The Cost of Persuasive Design.* 5Rights Foundation.
76. *Data Protection Act 2018.*
77. Information Commissioner's Office (2019). *Age-appropriate design: a code of practice for online services.*
78. *Children and Social Work Act 2017.*
79. UKCCIS (2018). *Education for a Connected World.*
80. PSHE Association (2018). *Health education and RSE guidance — the outstanding, the good and the 'requires improvement'.*
81. Department for Education (2019). *Relationships Education, Relationships and Sex Education, and Health Education in England: Government consultation response.*
82. Ofsted (2014). *Inspecting e-safety.*
83. Phippen, A. (2018). *UK Schools Online Safety Policy and Practice Assessment 2018.* South West Grid for Learning
84. Davidson, J. *et al.* (2016). *Enhancing Police and Industry Practice: EU Child Online Safety Project.*
85. Bond, E. *et al.* (2016). *Multi-agency E-safety Crime Prevention (MESCP) project.* Better Policing Collaborative.
86. NSPCC [online]. Keeping children safe online - online course. Accessed 25/07/19.
87. Marie Collins Foundation [online]. Click: Path to Protection. Accessed 25/07/19.
88. CEOP [online]. Ambassador Course. Accessed 25/07/19.
89. Internet Matters [online]. Guides & Resources. Accessed 25/07/19.
90. Childnet International [online]. Resources. Accessed 25/07/19.
91. Parent Zone [online]. For parents. Accessed 25/07/19.
92. NSPCC [online]. NSPCC and O2 - keeping children safe online. Accessed 25/07/19.
93. Thinkuknow [online]. Parents homepage. Accessed 25/07/19.
94. UK Safer Internet Centre [online]. Online Safety Live - free online safety events. Accessed 25/07/19.
95. UK Safer Internet Centre [online]. Professionals Online Safety Helpline. Accessed 25/07/19.
96. Welsh Assembly Government (2008). *Personal and social education framework for 7 to 19-year-olds in Wales.*
97. Welsh Government (2015). *Keeping Learners Safe.*
98. Department for Children, Education, Lifelong Learning and Skills (2008). *Information and communication technology in the National Curriculum in Wales : key stages 2-3.*
99. Welsh Government (2018). Digital Competence Framework.
100. Welsh Government [online]. New school curriculum: overview. Accessed 25/07/19.
101. Scottish Government (2016). *Technologies: Experiences and Outcomes.*
102. Scottish Government (2017). *National Action Plan on Internet Safety for Children and Young People.*
103. Northern Ireland Curriculum (2014). *The Northern Ireland Curriculum Primary.*
104. Northern Ireland Curriculum (2015). *The Statutory Curriculum at Key Stage 3.*
105. Northern Ireland Curriculum (2015). *Relationships and Sexuality Education Guidance.*
106. 5Rights Foundation *et al.* (2017). *Our Digital Rights.*
107. Childnet Digital Leaders Programme [online]. How it works. Accessed 25/07/19.
108. Ofcom (2014). *Ofcom Report on Internet safety measures.*
109. HM Government (2015). *Revised prevent duty guidance for England and Wales.*
110. Przybylski, A. K. *et al.* (2017). Internet Filtering Technology and Aversive Online Experiences in Adolescents. *J. Pediatr.*, Vol 184, 215-219.e1.
111. Open Rights Group (2018). *Age Verification - Risks and Recommendations.*
112. Phippen, A. (2015). Digital Rights and Pornography – A child protection catch-22 or lazy policy solutions? *OxPol.*
113. Muižnieks, N. (2014). Protecting children's rights in the digital world: an ever-growing challenge. *Commissioner for Human Rights, Human Rights Comment.*
114. *Digital Economy Act 2017.*
115. DCMS Press Release (2018). *£25m for 5G projects on the anniversary of the UK's Digital Strategy.*
116. Hansard HC (20/06/19), vol 662, col 368.
117. Open Rights Group (2019). *Age verification security standard analysis.*
118. BBFC (2018). *Guidance on Age-verification Arrangements.*