Inspecting e-safety in schools

Briefing for section 5 inspection

This briefing aims to support inspectors in reviewing school’s safeguarding arrangements when carrying out section 5 inspections.

Age group: All

Published: January 2014

Reference no: 120196

The Office for Standards in Education, Children's Services and Skills (Ofsted) regulates and inspects to achieve excellence in the care of children and young people, and in education and skills for learners of all ages. It regulates and inspects childcare and children's social care, and inspects the Children and Family Court Advisory Support Service (Cafcass), schools, colleges, initial teacher training, work-based learning and skills training, adult and community learning, and education and training in prisons and other secure establishments. It assesses council children’s services, and inspects services for looked after children, safeguarding and child protection.

If you would like a copy of this document in a different format, such as large print or Braille, please telephone 0300 123 1231, or email enquiries@ofsted.gov.uk.

This publication is available at www.ofsted.gov.uk/resources/120196.

To receive regular email alerts about new publications, including survey reports and school inspection reports, please visit our website and go to ‘Subscribe’.

Piccadilly Gate
Store St
Manchester
M1 2WD

T: 0300 123 1231
Textphone: 0161 618 8524
E: enquiries@ofsted.gov.uk
W: www.ofsted.gov.uk

No. 120196

Contents

Introduction

1. In the context of an inspection, e-safety may be described as the school's ability:

   - to protect and educate pupils and staff in their use of technology
   - to have the appropriate mechanisms to intervene and support any incident where appropriate.

2. The breadth of issues classified within e-safety is considerable, but can be categorised into three areas of risk:

   - **content:** being exposed to illegal, inappropriate or harmful material
   - **contact:** being subjected to harmful online interaction with other users
   - **conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

Background

3. In 2007 the government commissioned from Dr Tanya Byron a review of the risks that children face when using the internet and video games. Following publication of the review in 2008, Ofsted was asked, among other things, to evaluate the extent to which schools teach pupils to adopt safe and responsible practices in using new technologies. *The safe use of new technologies*[1] also assessed training on internet safety for the staff in the schools visited and considered the schools' links with families in terms of e-safety. The report had a number of key findings:

   - In the five schools where provision for e-safety was outstanding, all the staff, including members of the wider workforce, shared responsibility for it. Assemblies, tutorial time, personal, social, health and education lessons, and an age-appropriate curriculum for e-safety all helped pupils to become safe and responsible users of new technologies.
   - Pupils in the schools that had 'managed' systems had better knowledge and understanding of how to stay safe than those in schools with 'locked down' systems. Pupils were more vulnerable overall when schools used locked down systems because they were not given enough opportunities to learn how to assess and manage risk for themselves.
   - In the outstanding schools, senior leaders, governors, staff and families worked together to develop a clear strategy for e-safety. Policies were reviewed regularly in the light of technological developments. However, systematic review and evaluation were rare in the other schools visited.

[1] *The safe use of new technologies* (090231), Ofsted, 2010; www.ofsted.gov.uk/resources/090231.

- The outstanding schools recognised that, although they had excellent relationships with families, they needed to keep developing these to continue to support e-safety at home.
- Few of the schools visited made good use of the views of pupils and their parents to develop their e-safety provision.
- In some schools there were weaknesses in e-safety where pupils were receiving some of their education away from the school site.
- The weakest aspect of provision in the schools visited was the extent and quality of their training for staff. It did not involve all the staff and was not provided systematically. Even the schools that organised training for all their staff did not always monitor its impact systematically.

Recommendations for schools

4. The report recommended that schools:

- audit the training needs of all staff and provide training to improve their knowledge of and expertise in the safe and appropriate use of new technologies
- work closely with all families to help them ensure that their children use new technologies safely and responsibly both at home and at school
- use pupils' and families' views more often to develop e-safety strategies
- manage the transition from locked down systems to more managed systems to help pupils understand how to manage risk; to provide them with richer learning experiences; and to bridge the gap between systems at school and the more open systems outside school
- provide an age-related, comprehensive curriculum for e-safety that enables pupils to become safe and responsible users of new technologies
- work with their partners and other providers to ensure that pupils who receive part of their education away from school are e-safe
- systematically review and develop their e-safety procedures, including training, to ensure that they have a positive impact on pupils' knowledge and understanding.

Common risks inspectors are likely to encounter

5. Please note that this is not an exhaustive list.

Content

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites

- content validation: how to check authenticity and accuracy of online content

Contact

- grooming
- cyber-bullying in all forms
- identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self generated indecent images)
- copyright (little care or consideration for intellectual property and ownership – such as music and film)

Why is this important?

6. Technology offers unimaginable opportunities and is constantly evolving. Access is currently becoming universal and increasingly more mobile, and pupils are using technology at an ever earlier age, as illustrated below.

- Older children are spending more time online, and are more likely to go online alone. While children aged 5–15 continue to spend most time watching TV, children aged 12–15 are spending more time online (rising from 14.9 hours a week in 2011 to 17.1 in 2012) and now spend as much time in a week using the internet as they do watching television. They are also more likely than they were in 2011 to mostly use the internet in their bedrooms (43% in 2012 compared to 34% in 2011). Children who use the internet mostly alone comprise one in seven internet users aged 5–7 (14%), one in four aged 8–11 (24%) and over half of those aged 12–15 (55%).[2]
- Children are going online via a wider range of devices. Internet access via a PC, laptop or netbook is increasingly being supplemented by access via other devices. All age groups are more likely in 2012 to go online using a tablet computer, and children aged 5–7 and 12–15 are also more likely to go online using a mobile phone.[3] Children aged 5–7 are also less likely than in 2011 to go online using a PC, laptop or netbook (58% in 2012 compared to 65% in 2011). Children of all ages continue to use social networking

[2] OFCOM Children and Parents: Media Use and Attitudes Report, Oct 2012.
[3] OFCOM Children and Parents: Media Use and Attitudes Report, Oct 2012.

sites; 22% of those aged 8–11 and 80% of those aged 12–15, with those aged 8–11 having an average of 92 'friends' and 286 for 12–15 year olds[4].

7. Technology use and e-safety issues go hand in hand. Many incidents happen beyond the physical geography of the school and yet can impact on pupils or staff.

- 40% of Key Stage 3 and 4 students have witnessed a 'sexting' incident and, in the same group, 40% didn't consider topless images inappropriate.[5]
- 28% of Key Stage 3 and 4 students have been deliberately targeted, threatened or humiliated by an individual or group through the use of mobile phones or the internet. For over a quarter of these, this experience was ongoing, meaning that the individual was continuously targeted for bullying by the same person or group over a sustained period of time.[6]
- Issues are magnified for 'vulnerable' children (for example disabled pupils and those who have special educational needs, looked after children); the internet bypasses normal safeguarding procedures thus making children who are adopted or fostered at greater risk of having their identities discovered. This could be by their birth parents searching for them or themselves wanting to discover who their birth parents are.
- Girls are more likely than boys to be bullied online. Around 4% of those aged 8–11 and 9% of those aged 12–15 who use the internet say they have had experience of being bullied online in the past year. As with bullying through a mobile phone, this incidence has not changed for those aged 8–11 or 12–15 since 2011. Girls aged 12–15 are more likely than boys to say they have been bullied online in the past year (13% in 2012 compared to 5% in 2011)[7].
- Pupils with special educational needs are 16% more likely to be victims of online abuse; children from lower socio-economic groups are 12% more likely[6].

8. Just because these environments are online make them no less susceptible to potential harm compared to the physical world. This makes it vitally important that pupils and staff are fully prepared and supported to use these technologies responsibly.

[4] OFCOM Children and Parents: Media Use and Attitudes Report Oct, 2012.

[5] *Sharing personal images and videos among young people,* SWGfL & Plymouth University, 2009; http://www.swgfl.org.uk/Staying-Safe/Sexting-Survey.

[6] *Virtual Violence II*, Beatbullying, 2012; http://www.beatbullying.org/pdfs/Virtual-Violence-II.pdf.

[7] OFCOM Children and Parents: Media Use and Attitudes Report Oct, 2012.

Key features of good and outstanding practice

Whole school consistent approach	All teaching and non-teaching staff can recognise and are aware of e-safety issues. High quality leadership and management make e-safety a priority across all areas of the school (the school may also have achieved a recognised standard, for example the e-Safety Mark). A high priority given to training in e-safety, extending expertise widely and building internal capacity. The contribution of pupils, parents and the wider school community is valued and integrated.
Robust and integrated reporting routines	School-based reporting routes that are clearly understood and used by the whole school, for example online anonymous reporting systems. Report Abuse buttons, for example CEOP. Clear, signposted and respected routes to key members of staff. Effective use of peer mentoring and support.
Staff	All teaching and non-teaching staff receive regular and up-to-date training. One or more members of staff have a higher level of expertise and clearly defined responsibilities.
Policies	Rigorous e-safety policies and procedures are in place, written in plain English, contributed to by the whole school, updated regularly and ratified by governors. The e-safety policy should be integrated with other relevant policies such as behaviour, safeguarding and anti-bullying. The e-safety policy should incorporate an Acceptable Usage Policy that is understood and respected by pupils, staff and parents.
Education	An age-appropriate e-safety curriculum that is flexible, relevant and engages pupils' interest; that is used to promote e-safety through teaching pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety. Positive rewards are used to cultivate positive and responsible use. Peer mentoring programmes.
Infrastructure	Recognised Internet Service Provider (ISP) or Regional Broadband Consortium (RBC) together with age-related filtering that is actively monitored.
Monitoring and Evaluation	Risk assessment taken seriously and used to good effect in promoting e-safety. Using data effectively to assess the impact of e-safety practice and how this informs strategy.
Management of Personal Data	The impact level of personal data is understood and data is managed securely and in accordance with the statutory requirements of the Data Protection Act 1998.

	Any professional communications between the setting and clients that utilise technology should: • take place within clear and explicit professional boundaries • be transparent and open to scrutiny • not share any personal information with a child or young person.

Indicators of inadequate practice

- Personal data is often unsecured and/or leaves school site without encryption.
- Security of passwords is ineffective, for example passwords are shared or common with all but the youngest children.
- Policies are generic and not updated.
- There is no progressive, planned e-safety education across the curriculum, for example there is only an assembly held annually.
- There is no internet filtering or monitoring.
- There is no evidence of staff training.
- Children are not aware of how to report a problem.

Annex 1. Sample questions for school leadership

9. How do you ensure that all staff receive appropriate online safety training that is relevant and regularly up to date?

Why this question?	The Ofsted report *The safe use of new technologies*[8] (February 2010) concluded that staff training is a weak area of online safety provision. The South West Grid for Learning (SWGfL) report *Online Safety Policy and Practice*[9] concluded, based on feedback from 1500 UK schools via '360 degree safe', that staff training is consistently the weakest area of schools provision.
What to look for?	■ at least annual training (in-service or online) for all staff ■ training content updated to reflect current research and advances in technology ■ recognised individual or group with e-safety responsibility
What is good or outstanding practice?	■ one or more members of staff have a higher level of expertise and clearly defined responsibilities

10. What mechanisms does the school have in place to support pupils and staff facing online safety issues?

Why this question?	SWGfL concluded in their sexting survey (November 2009)[10] of 1,100 11–16 year olds, that 74% would prefer to report issues to their friends rather than a 'trusted adult'. The Department or Education (DfE) report *The use and effectiveness of anti-bullying strategies* (April 2011)[11] refers to multiple reporting routes, consistent whole school approach, good auditing processes and regular self-evaluation.
What to look for?	■ robust reporting channels

[8] *The safe use of new technologies (090231),* Ofsted, 2010; http://www.ofsted.gov.uk/resources/safe-use-of-new-technologies.

[9] *Online safety policy and practice in the UK and internationally – An analysis of 360 degree safe/Generation Safe self review data 2011*, SWGfL & Plymouth University, 2012, http://www.swgfl.org.uk/Staying-Safe/Files/Documents/Online-Safety-Policy0-and-Practice-in-the-UK-and-in.

[10] *Sharing personal images and videos among young people*, SWGfL & Plymouth University, 2009; http://www.swgfl.org.uk/Staying-Safe/Sexting-Survey.

[11] *The use and effectiveness of anti-bullying strategies in schools*, Department for Education (DfE), 2011; https://www.education.gov.uk/publications/eOrderingDownload/DFE-RR098.pdf.

What is good or outstanding practice?	■ online reporting mechanism, nominated members of staff, peer support

11. How does the school educate and support parents and whole school community with online safety?

Why this question?	Marc Prensky (2001)[12] coined the expression, 'digital natives' and 'digital immigrants', describing the 'generational digital divide' (Byron 2008)[13] that exists between children and their parents. Only 33% of European parents had filtering software on their computers.[14]
What to look for?	■ Parents' e-safety sessions ■ raising awareness through school website or newsletters
What is good or outstanding practice?	■ workshops for parents ■ regular and relevant e-safety resources offered to parents ■ children educating parents

12. Does the school have e-safety policies and acceptable use policies in place? How does the school know that they are clear and understood and respected by all?

Why this question?	The SWGfL report *Online safety policy and practice*[15] concluded that most schools consistently report having such policies in place, however very few have policies that are produced collaboratively, are linked to other policies, and are reviewed frequently.
What to look for?	■ e-safety policy is regularly reviewed ■ evidence that these are freely available (poster, handbooks, etc)

[12] Digital Natives, Digital Immigrants – A new way to look at ourselves and our kids; Marc Prensky, 2001; http://marcprensky.com/articles-in-publications/

[13] *Safer children in a digital world: the report of the Byron Review* (PP/D16(7578)/03/08), DCSF and DCMS, 2008; http://www.education.gov.uk/ukccis/about/a0076277/the-byron-reviews.

[14] Livingstone, Olafsson, O'Neill & Donoson, *Towards a better internet for children*, London School of Economics (LSE) 2012; http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20Online%20reports.aspx

[15] *Online safety policy and practice in the UK and internationally – An analysis of 360 degree safe/Generation Safe self review data 2011*, SWGfL & Plymouth University, 2012.

	■ children can recall rules
What is good or outstanding practice?	■ children integral to policy production

13. Describe how your school educates children and young people to build knowledge, skills and capability when it comes to online safety? How do you assess its effectiveness?

Why this question?	A key recommendation in the Byron review (2008)[16] was building the resilience of children to online issues through progressive and appropriate education.
What to look for?	■ planned and progressive e-safety education programme delivered across all age groups
What is good or outstanding practice?	■ e-safety is embedded throughout the school curriculum and is regularly reviewed

[16] *Safer children in a digital world: the report of the Byron Review* (PP/D16(7578)/03/08), DCSF and DCMS, 2008.

Annex 2. Sample questions for pupils

1. If you felt uncomfortable about anything you saw, or if anybody asked you for your personal details such as your address on the internet would you know where to go for help?
2. If anybody sent you hurtful messages on the internet or on your mobile phone would you know who to tell?
3. Can you tell me one of the rules your school has for using the internet?
4. Can you describe the risks of posting inappropriate content on the internet?

Annex 3. Sample questions for staff

1. Have you had any training that shows the risks to your and pupils online safety?
2. Are there policies in place that clearly demonstrate good and safe internet practice for staff and pupils?
3. Are there sanctions in place to enforce the above policies?
4. Do all staff understand what is meant by the term cyber-bullying and the effect it can have on themselves and pupils?
5. Are their clear reporting mechanisms with a set of actions in place for staff or pupils who feel they are being bullied online?
6. Does the school have any plans for an event on Safer Internet Day? (This is an annual event, now in its fifth year at least, so schools that participate will know about the event).

In a good school we should expect positive answers to all of the above. It would demonstrate a schools commitment to e-safety if all staff had received some awareness training outlining what the current risks are and what resources are available to help them keep pupils and themselves safe online.

Annex 4. Content, contact and conduct exemplars[17]

	Commercial	Aggressive	Sexual	Values
Content (child as recipient)	advertisements spam sponsorship personal information	violent/hateful content lifestyle sites	pornographic or unwelcome sexual content	bias racist misleading information or advice
Contact (child as participant)	tracking harvesting personal information	being bullied, harassed or stalked	meeting strangers being groomed	self-harm unwelcome persuasions
Conduct (child as actor)	illegal downloading hacking gambling financial scams terrorism	bullying or harassing another	creating and uploading inappropriate material; sexting	providing misleading info and advice health and wellbeing; time spent online

[17] Livingstone, Sonia and Haddon, Leslie, *'EU Kids Online: Final Report'*, LSE, 2009; http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20Online%20reports.aspx.

Annex 5. Current trends with technology use amongst children

Over one in three 3–4 year-olds use the internet. Ofcom Media research findings indicate that 37% use the internet via a PC, laptop or netbook, 6% via a tablet computer, and 3% via a mobile phone. Only 2% use a games console or games player to go online, and 2% use a portable media player; only 5% of this group have ever played games online. In terms of other devices, 44% use a games console or player and 9% use a tablet computer (including the 6% who use this to go online)[18].

Ofcom also found that children express high levels of confidence online: 83% of those aged 8–11 and 93% of those aged 12–15 say that they are confident that they know how to stay safe online, and this has remained stable over time. However, confidence and due caution do not necessarily go hand in hand - for example, using social networking sites to communicate with people not directly known to the child is more likely now than in 2011, both for those aged 8–11 (25% in 2012 compared to 12% in 2011) and those aged 12–15 (34% in 2012 compared to 24% in 2011).[19]

Research by EU Kids Online[20] finds that 'Internet use is increasingly individualised, privatised and mobile' and this is particularly true for the UK. This makes education and awareness interventions and materials critical, as children need to be empowered to make good decisions whenever and wherever they are using the internet. Compared to their European counterparts, UK children are more likely to access the internet from laptops, televisions, mobile phones, handheld devices and games consoles, and on average use 3.5 different devices to go online across four locations.[21]

However, supervising 'digital natives' can be difficult. Forty–six per cent of parents agree with the statement: 'my child knows more about the internet than I do'. Agreement increases with each age group: 22% of parents of those aged 5–7; 35% of parents of those aged 8–11; and 67% of parents of those aged 12–15. In addition, 54% of those aged 12–15 say that they know how to delete their online history and 26% say they have done this in the last year. Twenty-two per cent say they know how to disable any online filters or controls, while 8% say they have done this in the last year. [22]

[18] OFCOM Children and Parents: Media Use and Attitudes Report, Oct 2012.

[19] OFCOM Children and Parents: Media Use and Attitudes Report, Oct 2012. http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/oct2011/Children_and_parents.pdf

[20] *EU Kids Online II: Enhancing knowledge regarding European children's use, risk and safety online*, LSE, 2011; http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20Online%20reports.aspx.

[21] Livingstone, Sonia; *Risks and safety on the internet: the UK report*, LSE, 2010; http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/ParticipatingCountries/uk.aspx.

[22] OFCOM Children and Parents: Media Use and Attitudes Report, Oct 2012.

Ofcom[23] has revealed that in 2010, smartphone ownership reached 3% of those aged 5–7, 13% of those aged 8–11 and 35% of those aged 12–15 in the UK. By 2011, almost half of all young people aged 12–15 had a smartphone (47%). Ninety per cent of children aged 5–15 in the UK live in a household with a fixed or portable games console. This is often in a private location: nearly 50% of children aged 5–7 have a games console in their bedroom, rising to 70% of those aged 8–15. These devices are increasingly used to access the internet and play against others online: 20% of children aged 8–11 and nearly 25% of those aged 12–15 go online using a games console. Of boys aged 12–15 who play games, 19% say they mostly play with other people over the internet.

The EU Kids Online[24] project shows that schoolwork is the top online activity for UK youth (92% of those aged 9–16) and more than half of UK teachers believe that children with no internet access are seriously disadvantaged in their education (TES, 2010).[25] RaceOnline[26] evidence demonstrates that children with internet access at home attain higher exam results by two grades.

After schoolwork, playing games is the second most popular activity (83% of those aged 9–16), followed by watching video clips (75% of those aged 9–16) and visiting social networking sites (71% of those aged 9–16).[27] Games are particularly popular with younger children, and it is often through games that children first start to use technology. Just over 33% of those aged 8–11 in the UK visit sites like YouTube, rising to 66% of those aged 12–15 (Ofcom, 2011).

Younger children are increasingly using social networking sites as evidenced by the rise of usage by those aged 5–7 in the UK from 7% in 2009 to 23% in 2010.[28] This is largely driven by sites like Club Penguin and Moshi Monsters rather than age-restricted sites like Facebook. However, Facebook remains enormously popular (96% of those aged 8–15 with an active social networking site profile use Facebook) and there are a significant number of underage users accessing sites like Facebook which have a minimum user age of 13. In the UK, it seems that starting secondary school at the age of 11 is a key trigger for underage social networking: 28% of those aged 9–10 have an SNS profile compared to 59% of those aged 11–12.[29] However, safety campaigns do seem to be successful: although those aged 9–12 are the most likely

[23] UK *children's media literacy*, Ofcom, 2011; http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/media-lit11/childrens.pdf.

[24] *EU Kids Online II*: Enhancing knowledge regarding European children's use, risk and safety online; LSE, 2011.

[25] *Lack of internet access puts poorest children at educational disadvantage,* TES, 2010; http://www.tes.co.uk/article.aspx?storycode=6036318.

[26] *Survive and Thrive*, RaceOnline, 2011; http://raceonline2012.org/sites/default/files/resources/survive__thrive_-_charity_sustainability_through_technology.pdf.

[27] *Risks and safety on the internet: the UK report*, LSE, 2010.

[28] *UK children's media literacy*, Ofcom, 2011.

[29] *Risks and safety on the internet: the UK report*, LSE, 2010.

in Europe to display an incorrect age, they also the most likely to keep their profile private.[30]

[30] Livingstone, Sonia and Ólafsson, Kjartan and Staksrud, Elisabeth, *Social networking, age and privacy*, LSE, 2011; http://eprints.lse.ac.uk/35849/.

Annex 6. Glossary

Acronyms and jargon are common place in technology and often obscure meaning and understanding. The following link provides access to a wide ranging glossary of technological terms in current use http://www.digizen.org/glossary/.

In addition, the following terms used in this document are explained below

360 degree safe	SWGfL's online self-review tool for school improvement in online safety www.360safe.org.uk.
Age related filtering	Differentiated access to online content managed by the school and dependent on age and appropriate need (commonly used providers include Smoothwall, Lightspeed, Netsweeper, RM).
AUP	Acceptable Use Policy
Byron Review	Professor Tanya Byron's seminal report from 2008, 'Safer Children in a Digital World' available at http://www.education.gov.uk/ukccis/about/a0076277/the-byron-reviews.
CEOP	Child Exploitation and Online Protection centre.
Cyber bullying	Bullying using technology such as computers and mobile phones.
Encryption	Computer programme that scrambles data on devices such as laptops and memory sticks in order to make it virtually impossible to recover the original data in event of the loss of the device; schools often use this to protect personal data on portable devices.
EPICT	European Pedagogical ICT Accreditation.
E-safety mark	Accreditation for schools reaching threshold levels within 360 degree safe through assessment by external assessor.
Frape	Short for 'Facebook rape', referring to when a Facebook user's identity and profile are compromised and used by a third party to cause upset.
Games Console	Examples include XBOX 360, Nintendo Wii, PlayStation 3, and Nintendo DS.
Grooming	Online grooming is defined by the UK Home Office as: 'a course of conduct enacted by a suspected paedophile, which would give a reasonable person cause for concern that any meeting with a child arising from the conduct would be for unlawful purposes'.
Hacker	Originally thought of as a computer enthusiast, but now a hacker is normally used to refer to computer criminals, especially those who break into other people's computer networks.
Impact level	Impact levels indicate the sensitivity of data and the associated protection required (see the government published HMG Security Policy Framework http://www.cabinetoffice.gov.uk/spf). The scheme uses five markings, which in descending order of sensitivity are: TOP SECRET, SECRET, CONFIDENTIAL, RESTRICTED and PROTECT. Most pupil or staff personal data that is used within educational institutions will come under the PROTECT classification, however some (for example the home

	address of a child (or vulnerable adult) at risk) will be marked as RESTRICT.
ISP	Internet Service Provider (a company that connects computers to the internet for a fee).
Lifestyle website	An online site that covertly advocates particular behaviours and issues pertaining to young and often vulnerable children for example anorexia, self-harm or suicide.
Locked down system	In a locked down system almost every website has to be unbarred before a pupil can use it. This keeps the pupils safe, because they can use only websites vetted by their teachers, the technicians or by the local authority, any other website has to be unbarred for a pupil to be able to use it, which takes up time, detracts from learning and does not encourage the pupils to take responsibility for their actions (note that a locked down system may be appropriate in an EYFS setting or in a special school).
Malware	Bad software or programs that damage your computer (viruses), steal your personal information (spyware), display unwanted adverts (adware) or expose your computer to hackers (Trojan horses).
Managed system	In a managed system the school has some control over access to websites and ideally offers age-appropriate filtering. Pupils in schools that have managed systems have better knowledge and understanding of how to stay safe than those in schools with locked down systems because they are given opportunities to learn how to assess and manage risk for themselves.
Phishing	Pronounced the same as ‘fishing’ this is an attempt to trick people into visiting malicious websites by sending emails or other messages which pretend to come from banks or online shops; the e-mails have links in them which take people to fake sites set up to look like the real thing, where passwords and account details can be stolen.
Profile	Personal information held by the user on a social networking site.
RBC	Regional Broadband Consortium, often providers of schools broadband internet connectivity and services in England, for example SWGfL, London Grid for Learning (LGfL).
Safer Internet Day	Initiated by the European Commission and on the second day, of the second week of the second month each year.
Sexting	Sending and receiving of personal sexual images or conversations to another party, usually via mobile phone messaging or instant messaging.
SGII	Self generated indecent images (often referred to as “sexting” – see above)
SHARP	Example of an anonymous online reporting mechanism (Self Help And Reporting Process).
SNS	Social networking; not the same as computer networking, social networking is a way of using the internet and the web to find and make friends and stay in touch with people.

Spam	An e-mail message sent to a large number of people without their consent, usually promoting a product or service (also known as Unsolicited Commercial Email (UCE) or junk email).
Trojan	A malware program that is not what it seems to be. Trojan horses pretend to be useful programs like word processors but really install spyware or adware or open up a computer to hackers.
Youtube	Social networking site where users can upload, publish and share video.

Further information

Publications by Ofsted

The safe use of new technologies (090231), Ofsted, 2010;
www.ofsted.gov.uk/resources/090231

Other publications

Safer children in a digital world: the report of the Byron Review
(PP/D16(7578)/03/08), DCSF and DCMS, 2008;
http://www.education.gov.uk/ukccis/about/a0076277/the-byron-reviews

Ofcom's response to the Byron Review, Ofcom, 2008;
http://stakeholders.ofcom.org.uk/market-data-research/other/telecoms-research/byron/

Websites

UK Council for Child Internet Safety (UKCCIS); http://www.education.gov.uk/ukccis/

Child Exploitation and Online Protection Centre (CEOP); http://ceop.police.uk/

UK Safer Internet Centre; http://www.saferinternet.org.uk/

Childnet International; http://www.childnet.com/

SWGfL (South West Grid for Learning); http://www.swgfl.org.uk/

Cybermentors; https://cybermentors.org.uk/

Parentzone; http://www.theparentzone.co.uk/