Safe and responsible use

Keeping children safe

How can we keep children safe online?

Schools have a responsibility to keep pupils safe. The Byron Review,[1] Ofsted and others have emphasised that the best way to achieve this is to teach pupils how to keep themselves safe. Think of pupils cycling to school: the pupils are exposed to risks which could otherwise be avoided, but these risks are balanced by a range of benefits (independence, health, environment, road congestion, etc.). We do all we can to outweigh the risks by teaching pupils to cycle well and safely.

The new computing curriculum goes beyond just teaching **e-safety**, and states that key stage 2 pupils should be taught to:

> *use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.*[2]

It's important to recognise that these requirements are a whole school responsibility. They should be taught across the curriculum and become part of the life of the school – this isn't just something for computing lessons.

By moving from a risk mitigation approach to a values-based approach that promotes the responsible use of technology, we can help develop the pupils' sense of moral responsibility and the 'grit' necessary for pupils to stand up for doing the right thing. Pupils will then be far better at coping with the challenges of secondary education and adolescence, and far less likely to fall prey to the more sinister aspects of the internet and other technologies.

What are the risks?

In *The Byron Review* Professor Tanya Byron outlined three broad categories of risk which children are exposed to through their use of digital technology: content, contact and conduct.

	Commercial	Aggressive	Sexual	Values
Content (child as recipient)	Adverts Spam Sponsorship Personal info	Violent/hateful content	Pornographic or unwelcome sexual content	Bias Racist Misleading info or advice
Contact (child as participant)	Tracking Harvesting personal info	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	Providing misleading info/ advice

[1] **Byron, T., *Safer Children in a Digital World: The Report of the Byron Review* (London: DCSF, 2008).**

[2] **National Curriculum in England, *Computing Programmes of Study* (Department for Education, 2013).**

Content

Children are naturally curious, and as teachers we hope to develop that curiosity – to establish a life-long love of learning. The Web has provided almost instant access to a wealth of information that pupils can access to further their learning and satisfy their curiosity.

Schools have effective filters that minimise exposure to inappropriate material in school, but this does not prevent pupils accessing such material outside of school, including on tablets or smartphones.

Both Bing and Google have safe-search modes (which can be locked in place) and these help prevent pupils from accessing particularly inappropriate content. In addition, a number of organisations have developed search engines targeted at children (for example www.swiggle.org.uk/), often through a combination of safe-search and custom-search tools in Google search.

Encourage parents to use the safe search filters on their search engine, and to request filtered internet access at home and on mobile devices, explaining how to do this and why it is a good idea.

But, even *with* filters in place, children may still encounter content that concerns them. Establish a 'no blame' culture in school so they feel they can alert you, or their parents, to such content. Many schools teach children to close the laptop, switch off the monitor or turn the tablet over if they find content they know they shouldn't see or that concerns them; again it's worth explaining this to parents and suggesting they do the same at home.

Byron identified commercialisation as another risk associated with exposing pupils to the internet. As teachers, we must help pupils to become discerning and critical about commercial aspects of the content they come across. For example, teach them about spam in email and how this can be filtered semi-automatically, as well as asking them to think about what sort of algorithms might be used in doing so.

Talk to pupils about advertising on the web and how this can be avoided through the use of browser plugins such as AdBlock, as well as the difference between sponsored and other results from search engines. It's also important to help pupils become aware of the difference between altruistically created content such as Wikipedia and many blogs, and content created with a perhaps hidden or implicit commercial purpose, e.g. apparently free online services that are sustained through using the user's data to help target advertising.

Contact

The new curriculum requires that pupils are taught who they can turn to if they have concerns over contact online. In most cases, pupils should talk to their parents or their teachers about such contact: if pupils report such concerns to you, this is likely to be covered by your safeguarding policy, so make sure you follow this carefully. Sometimes pupils might be too embarrassed to turn to either you or their parents, so it's worth introducing them to ChildLine and, in the case of key stage 2 pupils, CEOP (see Further resources).

Traditionally e-safety work in schools has included clear advice to children on not sharing personal information online. The curriculum includes this at key stage 1. Online privacy is an increasing matter of concern and there are broader issues here than 'stranger danger'. Pupils should be aware of their 'digital footprint', the data about them that is created by deliberately sharing content and through the automatic logging of all online activity. Whilst such logs are kept securely, many people are concerned about the uses to which such data could be put.

Classroom activity ideas

- Challenge older pupils to consider how algorithms can be designed to filter search results from a search engine to make them safe for children.
- Ask older pupils to think about the long-term implications of the data trails they leave behind them when they search the internet. Ask them to discuss: 'Who do you want to keep your data private from?' (From internet predators? From future employers? From the providers of search, internet and email services? From advertisers? From the school network manager? From government agencies?)

Conduct

The curriculum at key stage 1 requires that pupils learn to use technology 'respectfully'. At key stage 2 this is extended to 'responsibly', and pupils should also learn to recognise acceptable and unacceptable behaviour. Supporting children's moral development is a vital part of primary education, as well as a

statutory requirement for a school's curriculum and, as part of 'spiritual, moral, social and cultural development', an element of all Ofsted inspections.

Lawrence Kohlberg's stages of moral development[3] offers one model for thinking about this:

1. Obedience and punishment orientation (How can I avoid punishment?)
2. Self-interest orientation (What's in it for me?)
3. Interpersonal accord and conformity (The good boy/girl attitude)
4. Authority and social-order maintaining orientation (Law and order morality)
5. Social contract orientation (Do unto others...)
6. Universal ethical principles (Principled conscience)

Under this model, we would hope to see pupils taking increasing responsibility for their own moral and ethical decisions and behaviour whilst at primary school. If schools take moral education seriously, many aspects of pupils' inappropriate conduct using technology can perhaps be avoided, or their consequences reduced.

Cyber-bullying

Even in primary schools, cyber-bullying is a common problem. Whilst this is more likely to happen outside of school, it's common for both bully and victim to be members of the same class or school and the cause and consequences may often be connected to school. As with bullying in general, a clear zero tolerance message is vital, together with a culture in which this can be reported in the knowledge that swift and effective action will follow. Alongside this, it's worth building up pupils' resilience to off-hand, unintentionally hurtful remarks from others and some recognition that not every online disagreement or critical comment constitutes bullying.

Copyright

There are generous exemptions from much copyright legislation for clearly specified educational use, but it's still important to teach and show best practice in the use of copyright material. This includes children (and teachers!) properly acknowledging the source of content and respecting any associated licence terms.

Creative Commons (see Further resources) provide a range of licences that allow those who create work to license it for re-use under a range of different conditions. You can teach pupils about this approach to sharing online and show them how they can search for, acknowledge and re-use Creative Commons licensed content in their own work. Both Google and Bing image search allow results to be filtered to show just images that have been licensed in this way.

Pupils own the copyright in their own work including the work they produce in school. As teachers, we should respect this by seeking permission from pupils and their parents before publishing pupils' work online. Asking parents to license this use of their children's work might seem over the top, but it's important that pupils learn about their rights as well as their responsibilities.

Terms and conditions

It's important that pupils and teachers respect the terms and conditions of any websites or other online services that they use. The terms and conditions of most online services run to many pages, but when signing up for new services, or asking pupils to do so, it's well worth checking through the sections on any age-restrictions as well as those on copyright and data privacy. US-based companies are required to abide by American COPPA (Children's Online Privacy Protection Act) legislation, which prevents their storing personal data on under 13s without parental consent. Thus, many US-based internet services prohibit under 13s from using the service. Primary school pupils using these services would be doing so without the operators' permission, which might be considered in breach of the UK Computer Misuse Act. Some services, including Office 365 and Google Apps for Education, allow schools to create accounts on behalf of children. Other websites, such as Scratch, allow teachers to create multiple accounts in their own name and share these with pupils.

Passwords

As more and more aspects of pupils' learning and life are mediated through online systems, it's important that they learn to protect their own online identity and respect the online identity of others. The sooner pupils can memorise and type in their own password (even a simple, short one) the better. Later on, encourage pupils to use long passwords that can't easily be guessed (e.g. CorrectBatteryHorseStaple), to use different passwords for different sites or services and to change passwords regularly. Discourage pupils from sharing passwords with one another (as this is usually their only way to prove who they are in any online system) or with their parents; many difficulties could arise through one parent impersonating their son or daughter in an otherwise secure 'walled garden' environment such as a school VLE or learning platform.

[3] Kohlberg, L., *Essays on Moral Development: Vol. 2, The Psychology of Moral Development* (Harper & Row, 1984).

Time to turn off

Finally, discuss with your pupils the opportunity cost associated with screen time. Time spent using a computer is time not spent doing other things, such as reading a (paper-based) book, learning a musical instrument, playing in a team and socialising face-to-face with family and friends. Whilst digital technology is seen by many as transformative of so many aspects of learning and life, many would count it a great shame if it came to dominate childhood to a greater extent than it already has. Helping children to become more discerning users of technology, knowing when it would be useful, and when it might be more of a distraction, is perhaps also one of our responsibilities as teachers.

Further resources

- Byron, T., *Safer Children in a Digital World: The Report of the Byron Review* (DCFS, 2008), available at: http://webarchive.nationalarchives.gov.uk/20130401151715/http://www.education.gov.uk/publications/eOrderingDownload/DCSF-00334-2008.pdf.
- Childnet's SMART rules: www.kidsmart.org.uk/beingsmart/.
- Creative Commons, for information and free licences to use, available at: http://creativecommons.org/.
- 'Digital Literacy & Citizenship from the South West Grid for Learning', teaching resources, available at: www.digital-literacy.org.uk/Home.aspx.
- Ofsted: 'Inspecting safeguarding in maintained schools and academies – Briefing for section 5 inspections', available at: www.ofsted.gov.uk/resources/inspecting-safeguarding-maintained-schools-and-academies-briefing-for-section-5-inspections.
- Thinkuknow.co.uk (CEOP), information and teaching resources for keeping children safe online, available at: www.thinkuknow.co.uk/Teachers/.
- UK Safer Internet Centre, for information and teaching resources, available at: www.saferinternet.org.uk.
- UNCRC (United Nations Convention on the Rights of the Child), for information and training on children's rights, available at: www.ohchr.org/en/professionalinterest/pages/crc.aspx.