

FROM DIGITAL LITERACY FOR
PRIMARY TEACHERS SAVAGE + BARNETT
CRITICAL PUBLISHING.COM 2015

com/

apter

how
hers.

9 E-safety and digital safeguarding

lying:
ying_

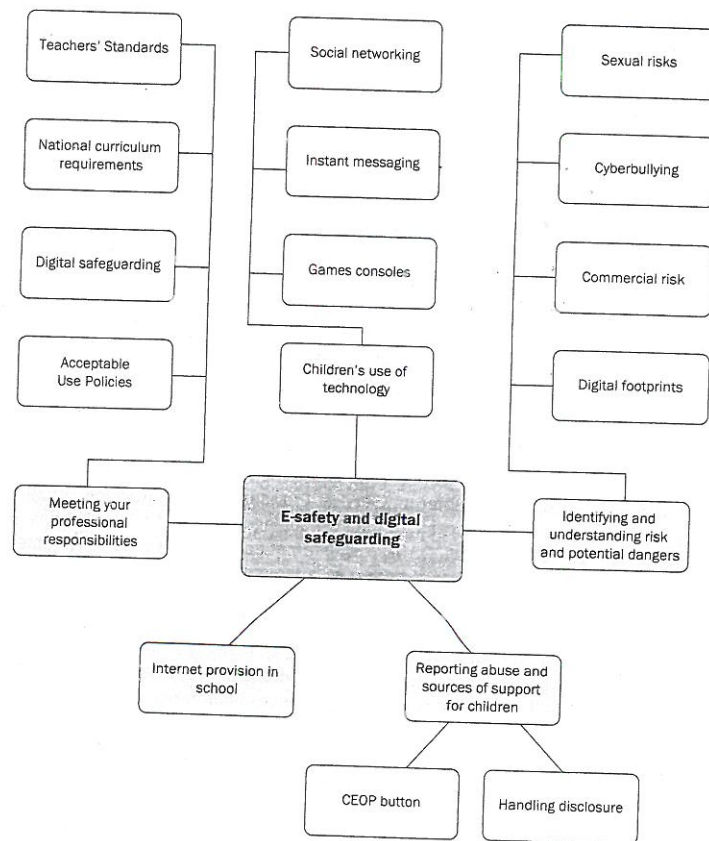
f and
ads/

L827

ers/

016-

ual_



Introduction

As a trainee or practising primary teacher the area of e-safety is challenging, evolving and complex. You will need to be aware of the vast range of technologies and online services children of primary age are using. These technologies change with trends and often have functional features that can create potential risks. How the profession and you as a trainee respond in terms of e-safety education requires careful consideration of a number of aspects; for example, balancing of risk and the need to inform and educate in relation to children's ages. Many aspects are problematic, for example, Facebook requires users to be 13 years of age but many teachers will know of children in their class who have an online profile on this or a similar social networking site whilst at primary school. A similar tension exists when considering how filtered access to the internet is within school compared to potentially open access at home. Your role may extend to educating parents about e-safety alongside children.

The first step in preparing yourself as a professional is to understand your responsibilities in relation to e-safety in terms of the Teachers' Standards and requirements of the computing programmes of study that come into place in September 2014. Your school setting will have policies and protocols that it is essential for you to locate and understand. Each school will have several policy documents including an Acceptable Use Policy relating to staff and pupil use of the internet on school premises, protocols for safeguarding pupil data and handling disclosures made by children. Always ensure you act in accordance with the agreed policies at the school you are working in and be aware that these may vary between your placement schools.

When you embark on e-safety education with children, preparation is essential. You need to be familiar with the technologies, benefits to learning, potential risks, be able to locate age-appropriate tried and tested resources and know how to handle a disclosure should this arise.

Internet provision in school

Schools will use a recognised Internet Service Provider (ISP) or Regional Broadband Consortium (RBC) to purchase access for their school; age-related filtering will be in place which is actively monitored (Ofsted, 2014, p 8). Internet access has evolved over time with many schools moving towards what is known as a managed system. Initially there was a temptation for schools to have locked down systems that were highly filtered and sanitised versions of the internet; sometimes sites could only be accessed if they had been unblocked one by one. On the one hand this was very reassuring for schools in terms of e-safety, however; one unforeseen consequence was that many educationally valid websites were blocked. Similarly, it was argued that in terms of e-safety education children were not being presented with a realistic experience similar to what they would face at home and this approach could in fact be putting children at greater risk. Hence, there has been a shift towards managed systems, negating some of the risks of accessing inappropriate material, and highlighting the importance of empowering children to understand risks and how to keep themselves safe. Ofsted reported that:

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.

(2014, p 4)

Meeting your professional responsibilities

In order to meet your professional responsibilities you need a clear understanding of: your role as detailed by the Teachers' Standards, the new national curriculum requirements, digital safeguarding protocols and key policy documents, for example, a school's Acceptable Use Policy.

Teachers' Standards

REFERS TO
ENG LAND HERE

Ofsted detail a school's e-safety responsibilities as 'to protect and educate pupils and staff in their use of technology' and 'to have the appropriate mechanisms to intervene and support any incident where appropriate' (2014, p 4). This underscores the principle that e-safety protocols and e-safety education is a responsibility of all trainees, teachers and adults working in a school and not just the computing subject leader or the domain of discrete computing sessions. Ofsted will look for a whole-school consistent approach (2014, p 8). Nor should you view e-safety education as a one-off topic, it should be an on-going process throughout Key Stages 1 and 2 and visited regularly, for example, via assemblies, pastoral time, personal, social and health education lessons (Ofsted, 2014, p 4). Technology is used across the curriculum and often class teachers are best placed to handle issues that are potentially sensitive with their learners as they know them best. As a trainee you should always talk with your class teacher about any plans you have for including e-safety aspects in your teaching. You will need to know about experiences they have had to date, whether there are any child protection issues or additional sensitivity required. Even when using well-established educational materials which are categorised by age you need to ensure you have viewed the materials in full in advance and discussed any concerns with your class teacher. You should be aware that access to technology and the internet can vary widely at home for the children in your care. Hopefully your plans will complement plans already in place at your school although you should be prepared to respond to queries or concerns as they arise. As soon as you begin visiting a new school placement ask to see the e-safety policy documents to ensure you are clear about the school's expectations of your professional conduct in relation to e-safety and safeguarding more generally. It would also be worth enquiring about any staff training opportunities whilst you are on placement and whether any parent education sessions are planned that you could attend whilst training at the school.

Your overarching aim should be to empower children to keep themselves safe by helping them to understand the benefits and risks involved with technology in a balanced and factually accurate way. Be truthful but not scaremongering and ensure there is always time for children to discuss and question both you and their peers. You should remember to include discussing the benefits to learning and leisure technology can bring and maintain perspective

on the dangers and risks. The goal is not to terrify or dissuade children from using technology but to enable them to make informed choices and manage risk. The Teachers' Standards, under which you must operate, make reference to 'having regard for the need to safeguard pupils' wellbeing' with respect to personal and professional conduct (DfE, 2011, p 10). A teacher's subject knowledge is crucial and again this is echoed in the Teachers' Standards in relation to having a secure knowledge of curriculum areas, keeping up to date and having a critical understanding of developments (DfE, 2011, p 7). Ultimately during training and post qualification these are your legal obligations as a professional. Keeping up to date requires career long continuing professional development and ideally this area of your expertise should be visited annually as technology and trends evolve. Ofsted has been critical about the 'extent and quality of training for staff in schools', specifically that it is often not systematic and the impact is not comprehensively monitored (2014, p 5). As this is such a crucial area you are strongly recommended to make the most of your school training by undertaking your own professional development activities starting with some of the resources suggested in this chapter.

National curriculum requirements *REFERENCE TO ENGLAND*

E-safety has been a priority area in primary education for several years and many professionals welcomed the explicit statements that have been included in the national curriculum 2014 programmes of study for computing. At Key Stage 1 pupils should be taught to: 'use technology safely and respectfully, keeping personal information private; know where to go for help and support when they have concerns about material on the internet' (DfE, 2013, p 189). Further at Key Stage 2 pupils should be taught to 'use technology safely, respectfully and responsibly; know a range of ways to report concerns and inappropriate behaviour' (DfE, 2013, p 189). It is crucial that you listen to the children in your care, their experiences and views as this will help ensure your e-safety education is relevant and will have impact. Data is available for national trends but within a locality, school, class or sub-group particular software applications may well be favoured over others. Favourite websites spread quickly amongst groups as there is a natural tendency for children wanting to conform and fit in with their peers.

In summary, for you to be able to teach the e-safety components specified in the national curriculum, you must:

- be able to identify the technologies the children you are working with are typically using both at school and at home;
- have a good understanding of the functionality of these technologies and applications even if it is your preference not to use them personally in your professional or personal life;
- understand privacy settings and the notion of leaving a digital footprint when any data is shared online;
- be aware of the benefits and potential risks inherent in these technologies;
- be aware of how concerns can be reported as both a professional and as a child;

- be aware of netiquette, responsible and respectful online protocols and be able to model and communicate these to learners;
- have a mechanism, personally and within the school context, for keeping up to date.

Critical questions

- » How prepared are you to teach the e-safety components of the computing programmes of study listed above?
- » Identify any knowledge gaps you currently may have. Use this chapter and the suggested further reading and resources to ensure you have a sound grasp of the key areas listed.

Digital safeguarding

You should be aware of legal and school based procedures for the digital safeguarding of pupil data. You need to know how to legally and appropriately access, update, store and retrieve any digital data that identifies personal information about the children in your care both on and off school premises. Ofsted highlights the key area of management of personal data in inspection guidance based on the Data Protection Act 1998. Inadequate practice is detailed as where personal data is unsecured or not encrypted, especially if taken from the school site (2014, pp 8–9). Whilst there is a responsibility on schools to have clear protocols in place and ensure all staff are aware, as a visiting trainee you are recommended to make direct enquiries about what is permissible or not. One area where there is great variation between school practice is in relation to accessing and copying personal educational plans for children with special educational needs or disabilities (SEND).

Critical questions

- » What guidance have you already received at your training institution in relation to digital safeguarding protocols?
 - » In particular what do you know about:
 - gaining permission to take digital photographs, how to pixelate identifying features, etc;
 - accessing and storing pupil data?
- Generic guidance is often contained in course and placement handbooks. If you are unable to locate this information, it is a valid question to ask of your tutors.
- Each time you visit a school ask what personal information about children you are permitted to have access to, whether you are allowed to copy that information and remove it from school premises, and if you are to photograph and record children.

Acceptable Use Policies

The schools you visit will have a number of policies where e-safety may be highlighted, for example, behaviour, safeguarding and anti-bullying policies (Ofsted, 2014, p 8). As you read

through the following sections it should become clear to you why e-safety has a specific mention in these contexts. One key document you should ensure you gain access to and fully understand when starting at a new school is the Acceptable Use Policy (AUP). Each school must have their own AUP that details how internet services are provided within that setting, details of filtered or managed systems, key information for parents and guidelines for use by staff and pupils. A partnership approach involving teachers, children, governors and parents is key to developing mutual understanding. A key issue is whether these policies are updated regularly to take account of new technologies and trends. Importantly AUPs should point out positive uses of technology rather than being simply a list of don'ts (Becta, 2009, p 31).

Becta outlined basic principles for an AUP including:

- be clear and concise;
- reflect the setting;
- encourage end-user input;
- be written in a style and tone appropriate to the end-user;
- promote positive uses of new and emerging technologies;
- clearly outline acceptable and unacceptable behaviours when using technology and network resources provided by the school;
- clearly outline acceptable and unacceptable behaviours when using personal technologies on school premises or networks;
- clearly outline what network monitoring will take place;
- clearly outline the sanctions for unacceptable use;
- be regularly reviewed and updated;
- be widely, and regularly, communicated to all stakeholder groups.

(Becta, 2009, pp 30–2)

Critical questions

Critically evaluate the AUP of a school you have visited. These are often available online via the school's website.

- » Are the responsibilities of all parties made clear?
- » Are conduct expectations clear and are consequences for breach identified?
- » When was it last updated?
- » Are current trends in technology and application use reflected?
- » If you have the opportunity ask children what their understanding and opinion is.

During an inspection Ofsted may ask similar questions of pupils, for example: 'can you tell me one of the rules your school has for using the internet?' or 'can you describe the risks of posting inappropriate content on the internet?' (2014, p 13).

Identifying and understanding risk and potential dangers

Overview

This section of the chapter is designed to give you the basic information regarding risk necessary to meet your professional responsibilities; it is not exhaustive but will give you some insight into unfamiliar topics and a useful framework to organise your thinking. Sexual risk, cyberbullying and commercial risks are explored in some detail alongside an exploration of what is meant by a digital footprint and the positive and negative implications of this data trail.

In 2007 Dr Tanya Byron was commissioned by the UK government to undertake a comprehensive review on e-safety, in particular the internet and video games, and provide guidelines for industry and educational establishments amongst others. Byron 'approached classification of the online risks to children in terms of content, contact and conduct in line with a model developed by the EU Kids Online project' originally by Hasebrink et al published in 2007 (2008, p 4). Many national bodies have since adopted this classification of risk, for example, Ofsted classifies e-safety as encompassing three areas of risk: content, contact and conduct (2014, p 4):

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

Table 9.1 Opportunities and risks for children online

		Content: Child as recipient	Contact: Child as participant	Conduct: Child as actor
Opportunities	Education learning and digital literacy	Educational resources	Contact with others who share one's interests	Self-initiated or collaborative learning
	Participation and civic engagement	Global information	Exchange among interest groups	Concrete forms of civic engagement
	Creativity and self-expression	Diversity of resources	Being invited/inspired to create or participate	User-generated content creation
	Identity and social connection	Advice (personal/health/sexual etc)	Social networking, shared experiences with others	Expression of identity
Risks	Commercial	Advertising, spam, sponsorship	Tracking/harvesting personal information	Gambling, illegal downloads, hacking
	Aggressive	Violent/gruesome/hateful content	Being bullied, harassed or stalked	Bullying or harassing another
	Sexual	Pornographic/harmful sexual content	Meeting strangers, being groomed	Creating/uploading pornographic material
	Values	Racist, biased info/advice (eg, drugs)	Self-harm, unwelcome persuasion	Providing advice eg, suicide/pro-anorexia

Source: Livingstone, S., and Haddon, L. (2009) *EU Kids Online: Final Report*. LSE, London: EU Kids Online. Available at <http://eprints.lse.ac.uk/24372/>

The EU Kids Online model reproduced below provides a balanced overview of online risks and opportunities for children considering them in three possible roles: recipient, participant and actor. Considering these three roles encourages us to think beyond the child as the victim and consider how the child might be involved in, for example, cyberbullying. Encouragingly this multiple perspective is echoed in the terminology adopted in the new computing curriculum, ie children should be taught to be respectful and responsible users. Further, the risks identified were categorised as either commercial, aggressive, sexual or values by Livingston et al, giving a comprehensive matrix for thinking about e-safety.

Sexual risks

Sexual risks are often the dimension that reaches the headlines most frequently and can include:

- a child (recipient role) accessing, intentionally or unintentionally, materials which are pornographic or highly sexualised and not age appropriate;
- a child (participant role) having unwanted contact with strangers or known persons and being stalked or groomed. Grooming can be defined as 'a process by which a person prepares a child for abuse with the specific goal of gaining access to the child, their compliance and maintaining secrecy' (Craven et al, 2006). The grooming process itself can take a variety of forms including 'bribery, gifts, flattery, threats, blackmail, sexualised games and desensitisation via exposure pornographic materials and/or child abuse images online or using a webcam' (CEOP, 2014);
- a child (actor role) themselves creating, uploading and/or sharing inappropriate and/or sexual material including images online or via text known as 'sexting' or SGII (self generated indecent image). In particular, it is vital to explore with children that once an image is shared digitally it cannot be recalled or deleted when an action is regretted. The image could be static or recorded by either party using a webcam. If the image is of a third party this in itself has legal implications and may be part of cyberbullying activities (see discussion below).

Cyberbullying

The risk of aggressive online behaviour can also prove very traumatic for children and young adults. Many professionals will have heard of the term of cyberbullying and how new technologies can mean that bullying can take place 24 hours a day, seven days a week beyond the school day. A range of platforms may be utilised including mobile phones, websites, forums, social media and networking, making it key that you know how these applications and tools work even if you are not a user in your own personal life. Without this detailed knowledge you will not be able to easily fulfil your professional responsibility to educate children about them.

A particularly troubling dimension with cyberbullying is that the perpetrator can fairly easily remain hidden or anonymous to the victim; sometimes imitating another person. Combined with the anonymity dimension the time and space dynamics can be far-reaching, traumatic and terrifying for the victim with little opportunity for escape or respite. Teachers have also

been victims of cyberbullying and sensible precautions will be discussed in Chapter 10. Key to both children who are recipients of cyberbullying and those who are actors involved in the bullying, is education about what constitutes cyberbullying, preventative strategies, collecting evidence, reporting instances and potential consequences. Sometimes those initiating the cyberbullying may not think through the consequences of their actions initially and lack awareness of the devastating impact their actions may have on the recipient. Whilst bullying is not a new phenomenon, the scale and potential audience, alongside the disconnection from the physical world technology brings, means that as a trainee teacher you need to have an up-to-date awareness of the issue.

Beatbullying is an international charity seeking to support and educate about bullying, including cyberbullying, and defines it as '*when someone uses technology, like the internet or a mobile phone, to deliberately hurt, humiliate, harass, intimidate or threaten someone else*' (www.beatbullying.org). Further, cyberbullying can take many forms, including: '*unpleasant or threatening texts or emails, posting abusive messages online, posting humiliating or embarrassing videos or pictures online, spreading rumours, setting up or contributing to a hate site or group, imitating someone else and prank calling, texts or messages*' (www.beatbullying.org).

CASE STUDY

Cyberbullying dilemma

Whilst on placement, trainee Isla is approached by a Year 5 girl from her class at break time. The girl is upset as the previous evening she received a SMS text message on her mobile phone saying unkind things. The message did not say who it was from and she did not recognise the number. She has been worrying about who has sent it and whether it is someone she knows at school. She deleted the message but is worried there might be another one tonight.

Critical questions

- » Is this a case of cyberbullying?
- » What criteria would you use to help you decide?
- » What initial advice would you give the child?
- » What follow-up actions would you take?

The Thinkuknow Cybercafe resource at www.thinkuknow.co.uk/8_10/cybercafe/Cyber-Cafe-Base/ contains a number of text message scenarios that may help you decide on your responses.

Commercial risks

Commercial risks to children are often overlooked but you need to be able to support children in understanding the possible risks and how to respond appropriately. The internet

often requires age information when signing up on sites however the lack of viable checks often lead children to sign up as older than they actually are. Anybody with an email address is familiar with the volume of spam and unsolicited mail received. You need to provide children with some informed guidance about illegal downloading sites and the potential consequences. Copyright in relation to music and film in particular is an area where awareness-raising of ownership and intellectual property is needed. This topic was explored in Chapter 7. In relation to e-safety consider whether you are a good role model for the children you are working with.

Educating children to be critical of web-based information extends beyond everyday lessons and should cover whether material is biased, racist or prejudicial also. There is also a worrying occurrence of sites promoting self-harm or pro-anorexia for example. Whilst teenagers may be at the greatest risk some awareness amongst primary teachers seems sensible.

Digital footprints

Relevant to many of the potential dangers outlined in the previous section is helping children to understand that activity online leaves a digital footprint. From a positive perspective this provides an evidence trail when reporting abuse. On the negative side this means an individual loses ownership of a digital artefact, for example, a photo, when it is posted online as they cannot be certain another person has not saved a version.

An important strategy you need to educate children about is that a digital data trail exists that can be collated and shared with a responsible adult when reporting the problem. Children need to understand that whatever is said, posted, shared or written online leaves a digital footprint or trail that can be tracked. Once an image is published no one can be sure it has not been accessed and downloaded by another party. Many social networking profiles reveal information about a person's location, school attended, friends, hobbies, etc, and unless appropriate privacy settings are applied to restrict access, this information is essentially public. Educating parents about their own online profiles and what is revealed about their children is also important if you are involved in a parent education event (CEOP, 2014). A thought-provoking analogy from one of the CEOP videos features a young girl posting a photo and details about herself on an online profile and asking children to recognise that the real-world equivalent would be handing out a flyer of the same information to unknown members of the public. Your role as a teacher is to facilitate children understanding the real-world equivalent of some of their online behaviours. You also need to understand levels of risk that certain action or inaction may create and know how to effectively minimise risk without negating the many benefits involved with online social interaction.

Children's use of technology

Overview

This section gives an overview of research on the patterns of technology use by children of primary age and explores social networking, instant messaging and games consoles including communication functions.

Over time an increasing range of devices allow internet access, including laptops, tablet computers, smartphones, fixed and portable games consoles, televisions, PCs and other handheld devices. Previously many families may have relied upon children accessing the internet via the family computer located in a communal space; however, now these methods of access are greater, smaller, more portable and WiFi enabled. As a result a greater number of children may be accessing the internet more frequently and in private on devices that are personalised where they may be the sole user. These trends are likely to continue to grow. This presents problems for some adults, including parents and teachers, who may feel disconnected or less aware than the children they are responsible for. Ofcom in 2013 reported that only four in ten parents have parental controls installed at home and around half of parents perceive their child as knowing more about the internet than they do.

Some trainee and practising teachers reading this chapter will be in danger of thinking this discussion relates primarily to teenagers and only a small minority of older primary school children. However, data from Ofcom in 2013 suggest some surprising trends.

Children aged three to four years old:

- 28% use a tablet computer at home;
- 12% of this age range use a tablet computer to go online;
- 58% of this age range played games online at least weekly.

Children aged eight to eleven years old:

- 18% owned a smartphone;
- 18% owned a tablet computer;
- schoolwork/homework is the most commonly mentioned internet activity carried out at least weekly 75%, followed by games 54% and information 45%;
- making and receiving voice and video calls (Skype or Facetime) has increased to 10%;
- 5% photo sharing websites such as Flickr, Instagram and Snaphish;
- about 22% have an active profile on a social networking site such as Facebook, Bebo or MySpace;
- 83% of 8–11 year olds say they are confident about how to stay safe online;
- 4% say they have experienced online bullying in the last year;
- 17% say they use the internet mainly in their bedroom.

(Ofcom, 2013, pp 4–9)

Social networking

Popular social networking sites including Facebook, Twitter and Instagram allow users to create a profile. A profile can contain a range of personal information including combinations of: name, age, address, contact details, email address, phone numbers, photographs, likes,

dislikes, hobbies, links to or embedded photo albums or videos. When accessed via smart-phone devices the geo-location services, if enabled, can locate a user in time and space. Individuals can build up a friend list that typically contains a mix of people they know in the real world and those they only know in the virtual world. Usually only an email address is required to set up an account which makes it very easy to create false accounts. Friendship requests can be sent and received. What is particularly confusing to many children is the desire to be popular and amass a large friend list even if this involves people they do not know in the real world or have had limited contact with.

Key to using social networking sites in a safe way are privacy settings. By default these settings are often set on public when signing up and creating a profile. The user is actively required to change the settings themselves and may also need to do this for different functions within the site, for example, photo access and newsfeed updates, and to regularly check settings, as changes are fairly frequent on these platforms. Currently on Facebook privacy settings can be applied to who can access/see information about and updates posted and who can make contact. In relation to access settings, options include: public, friends, only me, close friend or family lists. Similarly basic or strict filtering can be applied to contact permissions alongside options such as everyone and friends of friends. A detailed understanding of the implications and nuances of each is important.

The concepts of *friends* and *to friend someone* have very unique and specific meanings in social networking terms and the implications need to be fully understood. Inviting someone, or accepting an invitation from a person, to add to a friend list means that individual will subsequently see everything on a profile, past and future, where the privacy setting has been set to *visible to friends*. Often children's friend lists contain a mixture of people they know in the real world and people they only know online. Another common privacy setting is *visible to friends of friends*, meaning that people not known to the owner can view their information and updates. This functionality could potentially mean a great deal of personal information could be harvested by an unknown person.

Facebook requires users to be 13, but other than entering an appropriate date of birth no other checks are in place. Facebook does have a Family Safety Centre at www.facebook.com/safety/ offering advice for parents and those working with children. Location based services on phones are often embedded in applications such as Facebook and locate an individual in time and space.

There are also social networking sites targeted at younger audiences, a popular example is Club Penguin (www.clubpenguin.com). Club Penguin offers children of all ages a range of games, activities and opportunities to chat with other users. The child uses a penguin avatar they can customise and earn coins by playing games. The site has some inbuilt safety features, including: live moderators and filtered chat, an ad-free environment and some parental tools. There are an estimated 300 million users of this Disney-owned site (CEOP, 2014, p 8).

Instant messaging

Instant messaging is about communicating in real time either within another application or using a specific tool. Instant messaging can allow file transfers including photographs and

become web chat when a webcam is attached and activated. When a webcam is being used it is important to be aware that images can be recorded and later manipulated. When using instant messaging children should be reminded that: it is not advisable to swap files when you don't know who the other person is; to use a screen name that is gender neutral; be choosy about who to include on their list of contacts; not to give personal details; and use the safety features of their instant messaging software, eg block or ignore unwanted contacts.

Games consoles

Some teachers and parents may be unaware that popular games consoles connect to the internet, allow contacts to be built and both synchronous and asynchronous discussion to take place. Children who are at home in a safe and relaxed environment can feel protected, have a false sense of security and let their guard down. There are also well-being considerations for teachers to be aware of such as gaming addiction, overuse and children self-reporting long hours of game playing the evening before.

Reporting abuse and sources of support for children

Ofsted's inspection guidance on e-safety enquires about a school's ability to '*have appropriate mechanisms to intervene and support any incident*' (2014, p 4). Further, a key feature of good or outstanding practice specifies robust and integrated reporting routines where school-based reporting routes via designated staff are clearly understood and used by the whole school, and there is effective use of peer mentoring and support including clearly sign-posted channels (Ofsted, 2014, p 8) such as report abuse buttons (eg CEOP). Inadequate practice would include children not being aware of how to report a problem (p 9). Sample questions for children are also included:

- *If you felt uncomfortable about anything you saw, or if anyone asked you for your personal details such as your address on the internet would you know where to go for help?*
- *If anybody sent you hurtful messages on the internet or on your mobile phone would you know who to tell?*

(Ofsted, 2014, p 13)

Critical question

A further question for staff and pupils directly relates to cyberbullying: 'are there clear reporting mechanisms with a set of actions in place for staff or pupils who feel they are being bullied online?' (Ofsted, 2014, p 14)

- » *Consider how children in your class would respond to these sample questions.*

Child Exploitation and Online Protection Centre (CEOP) button

One well-established reporting mechanism is via the Child Exploitation and Online Protection Centre (CEOP) Report Abuse button.

The CEOP button enables children and young people, parents, carers and professionals to report any concerns they may have about potential grooming and suspicious child sex offender activity online. It provides a direct line to report to CEOP.

(CEOP, 2014, p 3)

Children under 11 are encouraged to report to a trusted adult who can help them complete the online information (CEOP, 2014, p 3). Once the button has been pressed you are taken to a page where navigation can be chosen according to age or parent/carer status. If immediate help is needed calling 999 is recommended. There are also other sources of support available, for example Childline and Cybermentors, offering children the opportunity to obtain advice from other children who have undergone specialist training. Advice screens are written in a child-friendly way offering both further sources of information or a further button to make an actual report where details of the incident or concern will need to be completed.

CEOP add-ons are available for all internet browsers to facilitate children only ever being one click away from being able to report concerns and CEOP has its own Facebook page, www.facebook.com/clickceop. Instructions for adding the CEOP button to a school website can be obtained through the Thinkuknow website following registration.

Handling disclosure

For a trainee the thought of a child making a disclosure can be a nerve-racking time. Each school will have precise protocols in place including designated members of senior staff. You should always consult the school you are in for this information. The guidance included here is based on information provided in CEOP Ambassador training and is not meant to replace localised procedures but offer some generic common-sense advice in the event that your e-safety session brings forth an unexpected disclosure from a child.

Should a child make a disclosure directly to you:

- *keep calm;*
- *reassure the child;*
- *consider who else can hear;*
- *listen carefully;*
- *do not ask leading questions or promise confidentiality;*
- *inform the school's child protection officer (CPO) or deputy for safeguarding without delay;*
- *remember to record the child's words as accurately as possible as soon as you can. Time, date and sign the recording.*

(CEOP, 2014)

Critical points

Ofsted (2014) has a sample list of questions for all staff members that you as a trainee teacher need to be able to answer confidently and positively on each school placement.

- » Have you had any training that shows the risks to your pupils' online safety?
- » Are there policies in place that clearly demonstrate good and safe internet practice for staff and pupils?
- » Are there sanctions in place to enforce the above policies?
- » Do all staff understand what is meant by the term cyberbullying and the effect it can have on themselves and pupils?
- » Are there clear reporting mechanisms with a set of actions in place for staff or pupils who feel they are being bullied online?
- » Does the school have any plans for an event on Safer Internet Day? (This is an annual event, which has been going for some time, so schools that participate will know about the event.)

Further reading and useful resources

- Know IT All for Primary School Teachers 'is an award winning resource designed especially for primary school staff to help them understand important e-safety issues and how to get the most out of the internet': www.childnet.com/resources/know-it-all-for-primary.
- 'CEOP's Thinkuknow programme provides a range of free educational resources – films, lesson plans, presentations, practitioner guidance, games and posters – to professionals working with children and young people': www.thinkuknow.co.uk/.
- Cross et al reported that '16% of children with a Statement of Special Educational Needs, while no more likely than their peers to be cyber-bullied overall, are significantly more likely to be targets of persistent cyber-bullying (harassment that is repeated and ongoing over a period of weeks or months to years)' (2012, p 15). Targeted resources for use with children are available at KnowITAll for Teachers – SEN: www.childnet.com/resources/know-it-all-for-teachers-sen.
- The Beatbullying website also offers individualised support via the 'I need to talk' option with the options to access a cyber mentor for support, to send an urgent message to a counsellor or visit the support forum: www.beatbullying.org/about_this_site/what_is_cyberbullying/.

References

- Beatbullying (2014) What is Cyberbullying? [online] Available at: www.beatbullying.org/about_this_site/what_is_cyberbullying/ (accessed 31 October 2014).
- Becta (2009) *AUPs in Context: Establishing Safe and Responsible Online Behaviours*. [online] Available at: webarchive.nationalarchives.gov.uk/20101102103654/publications.becta.org.uk/display.cfm?resID=39286 (accessed 31 October 2014).

- CEOP (Child Exploitation and Online Protection Centre) (2014) www.thinkuknow.co.uk/Teachers/Training/paidtrainingdetails/ (accessed 5 November 2014).
- Child Exploitation and Online Protection Centre (2013) *Thinkuknow Introduction Script for Ambassadors*.
- Craven, S, Brown, S and Gilchrist, E (2006) Sexual Grooming of Children: Review of Literature and Theoretical Considerations. *Journal of Sexual Aggression*, 12(3): 287–99.
- Cross, E-J, Piggin, R, Douglas, T and Vonkaenal-Flatt, J (2012) *Virtual Violence II: Progress and Challenges in the Fight against Cyberbullying*. [online] Available at: www2.beatbullying.org/pdfs/Virtual-Violence-II.pdf (accessed 31 October 2014).
- Department for Children, Schools and Families, and the Department for Culture, Media and Sport (2008) *Safer Children in a Digital World: The Report of the Byron Review*. [online] Available at: webarchive.nationalarchives.gov.uk/20101021152907/http://publications.education.gov.uk/eorderingdownload/dcsf-00334-2008.pdf (accessed 31 October 2014).
- Department for Education (2011) *Teachers' Standards: Guidance for School Leaders, School Staff and Governing Bodies*. [online] Available at: www.gov.uk/government/uploads/system/uploads/attachment_data/file/208682/Teachers_Standards_2013.pdf (accessed 31 October 2014).
- Department for Education (2013) *The National Curriculum in England: Framework Document*. [online] Available at: www.gov.uk/government/uploads/system/uploads/attachment_data/file/210969/NC_framework_document_-_FINAL.pdf (accessed 31 October 2014).
- Hasebrink, U, Livingstone, S, Haddon, L, Kirwil, L and Ponte, C (2007) *EU Kids Go Online: Comparing Children's Online Activities and Risks across Europe*. LSE, London: EU Kids Online.
- Livingstone, S and Haddon, L (2009) *EU Kids Online: Final Report*. London School of Economics. [online] Available at: [www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20I%20\(2006-9\)/EU%20Kids%20Online%20I%20Reports/EUKidsOnlineFinalReport.pdf](http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20I%20(2006-9)/EU%20Kids%20Online%20I%20Reports/EUKidsOnlineFinalReport.pdf) (accessed 31 October 2014).
- Office of Communications (2013) *Children and Parents: Media Use and Attitudes Report*. [online] Available at: stakeholders.ofcom.org.uk/binaries/research/media-literacy/october-2013/research07Oct2013.pdf (accessed 31 October 2014).
- The Office for Standards in Education, Children's Services and Skills (2014) *Inspecting e-Safety in schools: Briefing for Section 5 Inspection*. Ref no: 120196.