Southend-on-Sea

LSCB

Local Safeguarding Children Board

E Safety and the Use of Social Media Handbook

October 2013

Contents

Section 1 - Guidance on Developing an E-Safety Policy

Page

Section 1 - Guidance on Developing an E-Safety Policy

1. Why do we need an e-safety policy?

Each new technology introduces new opportunities and challenges for children and young people, parents, carers and those working with young people. In order to minimise the risks involved from new technologies we need to understand how children and young people use ICT and how this may be misused by those who may present a risk to children. It is important that we know how to respond when concerns arise. For example, would you know how to respond if:

- A young person reported cyber bullying?
- A young person put images on a website containing sexually explicit material they had videoed on their mobile phone?
- A member of staff was found downloading pornography?
- A young person tells you they have arranged to meet someone who they met on line?
- You receive an inappropriate or illegal image by email?

In recent years the internet and other means of electronic communications have become increasingly accessible to children and young people, whether at school, in public libraries or in the home. This provides great opportunities for young people in terms of education, information, communication and having fun. However it also includes risks from those intent on sexually exploiting children and from the inappropriate use of communications technology. This highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology. It also highlights the need to provide appropriate guidance to those working with children and parents and carers.

All organisations providing services for children and young people have a responsibility to ensure that they understand e-safety issues, know how to help children stay safe online and have procedures in place to support those working with children in knowing how to respond when concerns arise.

Open access to the Internet has become an integral part of many children's lives and is an invaluable resource. However much of the material on the Internet is published for an adult audience and some is unsuitable for children and young people. In addition, there is information on weapons, crime and racism access to which would be more restricted elsewhere. In order to safeguard and promote the welfare of children all organisations need to work together to provide a coordinated e-safety strategy and this document aims to highlight key aspects to consider in developing e-safety policies and in ensuring these are effective.

What does electronic communication include?

- **Internet collaboration tools:** social networking sites and blogs
- **Internet Research**: web sites, search engines and Web browsers
- **Mobile Phones and personal digital assistants** (PDAs)
- **Internet communications:** e-Mail and instant messaging (IM)
- **Webcams and videoconferencing**

2. What is e-safety?

Abuse and neglect are forms of maltreatment of a child. Somebody may abuse or neglect a child by inflicting harm, or by failing to act to prevent harm. Children may be abused in a family or in an institutional or community setting or ***in an interactive communications technologies environment***; by those known to them or, more rarely, by a stranger. They may be abused by an adult or adults or another child or children.

We know that ICT can offer new weapons for bullies, who may torment their victims via websites or text messages.

Local Safeguarding Children Boards have an important role in co-coordinating and ensuring the effectiveness of local work to safeguard and promote the welfare of children. This guidance aims to support organisations in reviewing their own e-safety agenda and to help in developing effective e-safety polices and procedures.

3. What are the risks?

ICT can offer many positive educational and social benefits to young people, but unfortunately there are some dangers. As in any other area of life, children and young people are vulnerable and may expose themselves to danger, whether knowingly or unknowingly, when using the internet and other technologies. Additionally, some young people may find themselves involved in activities which are inappropriate, or possibly illegal.

Risks include:

Content

- Exposure to age-inappropriate material
- Exposure to inaccurate or misleading information
- Exposure to socially unacceptable material, such as that inciting violence, hate or intolerance
- Exposure to illegal material, such as images of child abuse.

Contact

- Grooming using communication technologies to meet and groom children with the intention of sexually abusing them (both on and off line exploitation).

Commerce

- Exposure of minors to inappropriate commercial advertising
- Exposure to online gambling services
- Commercial and financial scams

Copyright infringement

Copyright law applies on the internet, but is ignored by many young people who download and swap music files, cut and paste homework assignments from others' work, or even purchase whole assignments from online cheat sites without realising the implications and consequences. See the E-safety section on the Becta Schools website for further information on copyright http://www.becta.org.uk/schools/esafety].

Obsessive use of the internet and ICT

There is the potential for children and young people to become obsessed with the internet and related technologies. Factors such as spending a significant amount of time online, deterioration of the quality of school work, diminished sleep time, or negative impacts upon family relationships, may all be indicators that the internet is taking too high a priority in a young person's life.

Exposure to inappropriate materials

There is a risk that when using the internet, email or chat services, young people may be exposed to inappropriate material. This may be material that is pornographic, hateful or violent in nature, encourages activities that are dangerous or illegal, or is just age-inappropriate or biased. One of the key benefits of the web is that it is open to all, but unfortunately this also means that those with extreme political, racist or sexist views are able to spread their distorted view of the world.

In the case of pornography, there is no doubt that the internet plays host to a large amount of legal and illegal material. Curiosity about pornography is a normal part of sexual development, but young people may be shocked by some of the material online. It is not known what the long-term effects of exposure to such images may be.

Inappropriate or illegal behaviour

Young people may get involved in inappropriate, antisocial or illegal behaviour while using new technologies. Just as in the real world, groups or cliques can form online, and activities that start out as harmless fun, such as voicing an opposing opinion to another member of a chat room, can quickly escalate to something much more serious. Online bullying is an unfortunate aspect of the use of new technologies, perceived as providing an anonymous method by which bullies can torment their victims at any time of day or night. While a young person may not be in physical danger, they may receive email, chat or text messages that make them feel embarrassed, upset, depressed or afraid. This can damage their self-esteem and pose a threat to their psychological wellbeing. Some children and young people may become involved in much more serious activities. Possible risks include involvement in identity theft or participation in hate or cult websites, or the buying and selling of stolen goods. The ease of access to online gambling, suicide sites, sites for the sale of weapons, hacking sites, and sites providing recipes for drug or bomb making are also of great concern. Young people may also become involved in the viewing, possession, making and distribution of indecent and/or child pornographic images. Any concern relating to criminally obscene or criminally racist content can be reported to the Internet Watch Foundation or the police.

Physical danger and sexual abuse

The threat of physical danger is perhaps the most worrying and extreme risk associated with the use of the internet and other technologies. A criminal minority make use of the internet and related services such as chat rooms to make contact with young people.

The intention of these people is to establish and develop relationships with young people with the sole purpose of persuading them into sexual activity. Paedophiles will often target specific individuals, posing as a young person with similar interests and hobbies in order to establish an online 'friendship'. These relationships may develop over days or weeks, or even months or years, as the paedophile gains the trust and confidence of the young person, perhaps progressing to other forms of contact such as text messaging as a prelude to meeting in person. These techniques are often known as 'online enticement', 'grooming' or 'child procurement'.

The Sexual Offences Act 2003, which came into force in May 2004, includes a grooming offence specifically introduced to combat this abuse of the internet and young people. There is also a risk that while online a young person might provide information that can personally identify them or others, or arrange to meet people they have met online, so posing a risk to their safety or that of their family or friends.

Inappropriate or illegal behaviour by people working with children

Unfortunately, people working with children have also been found to have been involved in inappropriate or illegal behaviour relating to ICT use. This may include viewing or circulating inappropriate material via email, or much more serious activities such as viewing, possessing, making or distributing indecent and/or child pornographic images. Organisations also have a responsibility, therefore, to educate staff as to acceptable behaviours online, and to monitor networks for evidence of inappropriate activity. Inappropriate activity by a staff member may result in a disciplinary response. If illegal behaviour by a staff member is suspected, the organisation has a duty to consult with the police at the earliest opportunity, preserving any potential evidence.

The research evidence

In June 2006 68% of homes had internet access and in recent years there has been much research into children and young people's use of the internet and digital technologies. The UK Children Go Online (UKCGO) study offered a rigorous and timely investigation of 9–19 year olds' use of the internet between 2003 and 2005.

The study found the following:

- Access platforms are diversifying (71% have internet access via a computer, 38% via a mobile phone, 17% via a digital television and 8% via a games console)
- Most are daily (41%) or weekly (43%) users, with many children using the internet for searching and homework (90%)
- The internet can encourage participation (for example, 44% of 9–19 year old weekly users have completed a quiz online, 25% have sent an email or text message to a website, and 22% have voted for something online), and involvement in civic issues (54% of 12–19 year olds who use the internet at least weekly have used sites concerned with political or civic issues)

- The internet can also provide a source of advice (25% of 12–19 year old daily and weekly users say they go online to get advice)
- Contrary to public perception, there is little reported interest in contacting strangers online, and most online communication is with existing friends – and generally by mobile phone in preference to emailing or instant messaging.

However, the study also found the following:

- Children lack key skills in evaluating online content (38% of pupils aged between 9 and 19 trust most of the information on the internet, and only 33% of daily and weekly users have been taught how to judge the reliability of online information). See UK Children Go Online website www.children-go-online.net

(REF: BECTA: Safeguarding Children on line)

4. Objectives of an e-safety strategy

All organisations that work with children and young people need to have an e-strategy in place based on the following objectives:

1. *Ensuring that all children, young people & parents/carers are equipped with the knowledge and skills to safeguard themselves in the virtual world;*

2. *Ensure that all people who work with children & young people have access to effective policies and procedures and effective training to safeguard children at risk through online activity; and*

3. *Ensure that they know how to respond when concerns arise regarding the misuse of communications technology.*

Stakeholders

Organisations that need e-safety strategies include libraries, schools, post 16 and adult education, social care, looked after children: private fostering and children's homes, connexions, youth services, children's centres, youth offending service, probation, police, private ICT training centres, internet cafes, health, and the community and voluntary sector.

This document aims to provide information for organisations in helping them to develop e-safety policies.

Objective 1: ***Ensuring that all children, young people & parents/carers are equipped with the knowledge and skills to safeguard themselves in the virtual world;***

There is a great deal of information available to help children and young people stay safe on line, the following sites may help in developing an e safety policy:

www.thinnkuknow.co.uk

www.ceop.co.uk

www.parentcentre.co.uk

www.becta.co.uk

Parents and those working with children need to be aware that the Internet has online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even quite different interests. Guests can be invited to view personal spaces and leave comments, over which there may be limited control.

For use by responsible adults, social networking sites provide easy to use, free facilities; although often advertising intrudes and may be dubious in content.

Examples include: blogs, wikis, MySpace, Bebo, Piczo, Windows Live Spaces, MSN space, forums, bulletin boards, multi-player online gaming, chatrooms, instant messenger and many others.

Points to consider include:

- Children and young people who use social networking sites such as Bebo and Piczo need to learn that publishing personal information could compromise their security and that of others.
- Children and young people should be encouraged to think about the ease of uploading personal information and the impossibility of removing an inappropriate photo or address once published.
- They must not publish personal information, such as location and contact details.
- Consideration should be given to advising children to use an anonymous "cyber name" where logging into sites is essential.

E-safety education

Children and young people need to be educated in the responsible and safe use of the Internet and other technologies through a range of strategies including:

Think U Know training - Within Essex schools a number of staff have been trained to deliver this training and the ESCB has a list of professionals trained in other organisations.

The Becta leaflet “Signposts to Safety” discusses in detail how e-safety themes and ideas can be integrated in schools.

Information for parents

CEOP provide the following advice for parents

- Know what your children are doing online and who they are talking to. Ask them to teach you to use any applications you have never used.
- Keeping the computer in a family room means that you can share your child’s online experience – and that they are less likely to act inappropriately (i.e. via webcam).
- Help your children to understand that they should never give out personal details to online friends - personal information includes their messenger id, email address, mobile number and any pictures of themselves, their family or friends - if your child publishes a picture or video online - anyone can change it or share it. Remind them that anyone may be looking at their images and one day a future employer could!
- If your child receives spam / junk email & texts, remind them never to believe them, reply to them or use them.
- It's not a good idea for your child to open files that are from people they don't know. They won't know what they contain – it could be a virus, or worse - an inappropriate image or film.
- Help your child to understand that some people lie online and that therefore it's better to keep online mates online. They should never meet up with any strangers without an adult they trust.

- Always keep communication open for a child to know that it's never too late to tell someone if something makes them feel uncomfortable.
- Teach young people how to block someone online and report them if they feel uncomfortable.

Websites:

www.ceop.gov.uk

www.thinkuknow.co.uk

www.getnetwise.org

www.parentscentre.co.uk also suggests to parents:

1. Think about what software you can buy to protect children from viewing unsuitable or illegal content on the internet. OFCOM, the communications industry regulator, has worked with the British Standards Institute (BSI) to develop a BSI standard for internet content control software and the first kite marks are due out in 2007. This will help monitor the online activities of their children and help avoid children accessing illegal or inappropriate content.
2. Check out what child protection services your Internet Service Provider (ISP) offers - do they filter for spam, for instance? If not, ask them why.
3. Make up a family email address to receive the mail that does not include your name.
4. Children love to chat, but make sure they only use moderated chat rooms and encourage them to introduce you to their online friends.
5. Encourage your children to tell you if they feel uncomfortable, upset or threatened by anything they see online.
6. Involve your children in writing your own family code of acceptable internet use. Remember that what's acceptable for a teenager isn't necessarily ok for a primary school aged child, so get their input.

7. Computer kit is expensive so bear in mind that a child with a laptop may be vulnerable when carrying it to and from school.
8. The web's a great resource for homework but remember to use more than one site in research to get broad, balanced information and always reference your research sources.

Objective 2*: Ensure that all people who work with children & young people have access to effective policies and procedures and effective training to safeguard children at risk through online activity*

Advice on developing procedures for using the Internet

Most Internet use is safe, purposeful and beneficial to children. There is always an element of risk: even an innocent search can occasionally turn up links to adult content or violent imagery. For many children the greatest risk is through inadvertent access. Fast broadband means that inappropriate images can appear almost instantaneously. Children can innocently follow a series of links to undesirable content.

A procedure should be agreed on what to do, and how to handle the situation that may arise when working with children and young people. For example:

Close or minimise the image or window immediately. Don’t try to navigate away. If children saw the page, talk to them about what has happened, and reassure them.

Consider what supervision is appropriate when children are using the internet in your organisations setting.

When formulating your policy, consider:

- Who is responsible for the internet safety policies? Is there a nominated member of staff for coordinating all internet safety issues?
- Is there a regular risk assessment of your e-safety infrastructure?
- Is the policy consistent with the SET Child Protection Procedures?

- Is the policy supported by clear procedures should incidents of misuse occur? Are all staff aware of their individual responsibilities in responding to certain types of incident?
- Do you have an acceptable use policy that covers all relevant technologies?
- Is the policy regularly reviewed and updated?
- Are children involved in the creation of internet safety policies?
- Do you have filtering systems in place to prevent access to inappropriate materials? Are these systems regularly reviewed and updated. As a minimum all organisations should use an ISP who subscribes to the IWF filter list.
- Are children and young people aware of the procedures for reporting accidental access to inappropriate materials?
- Are there procedures in place regarding the deliberate access to inappropriate materials? Are children and young people aware of these?
- Are children and young people aware of their social responsibilities with regard to using the internet and related technologies, including treating others with respect?
- Consider adding www.thinkuknow.co.uk to favourites so that children and young people have a direct reporting line to CEOP.

(Adapted from BECTA checklists)

Developing filtering standards

It is important to use as a minimum an ISP who subscribes to the Internet Watch Foundation (IWF) filtering list. This will help to filter out some inappropriate content, but not all. Using an accredited Internet Service Provider (ISP) will also provide higher standards for filtering. The E-safety section of the Becta Schools website provides further information on internet filtering systems.

It is important to think about what search engines you use. If Google is to be used, you should/must make sure that strict filtering is applied. Go to ***www.google.co.uk*** and click Preferences.

The BBC search engine is an example of a safer approach for children: h***ttp://search.bbc.co.uk/***

Objective 3: *Ensure that they know how to respond when concerns arise regarding the misuse of communications technology.*

Response to an incident of concern

Internet technologies and electronic communications provide children and young people with the opportunity to broaden their learning experience and develop creativity in and out of school. However, it is also important to consider the risks associated with how these technologies are used.

These risks to e-safety are, of course, caused by people acting inappropriately or even illegally. Any potential issue must be dealt with at a personal level and observation is essential in being alert to concerns that children and young people may not report. Incidents will vary from the prank or unconsidered action to occasional extremely concerning incidents that may involve referrals to social care and Essex police (CAIU).

This section will help staff determine what action they can take when they identify concerns and should be read in conjunction with the SET Procedures www.southend.gov.uk/lscb.

How do we respond?

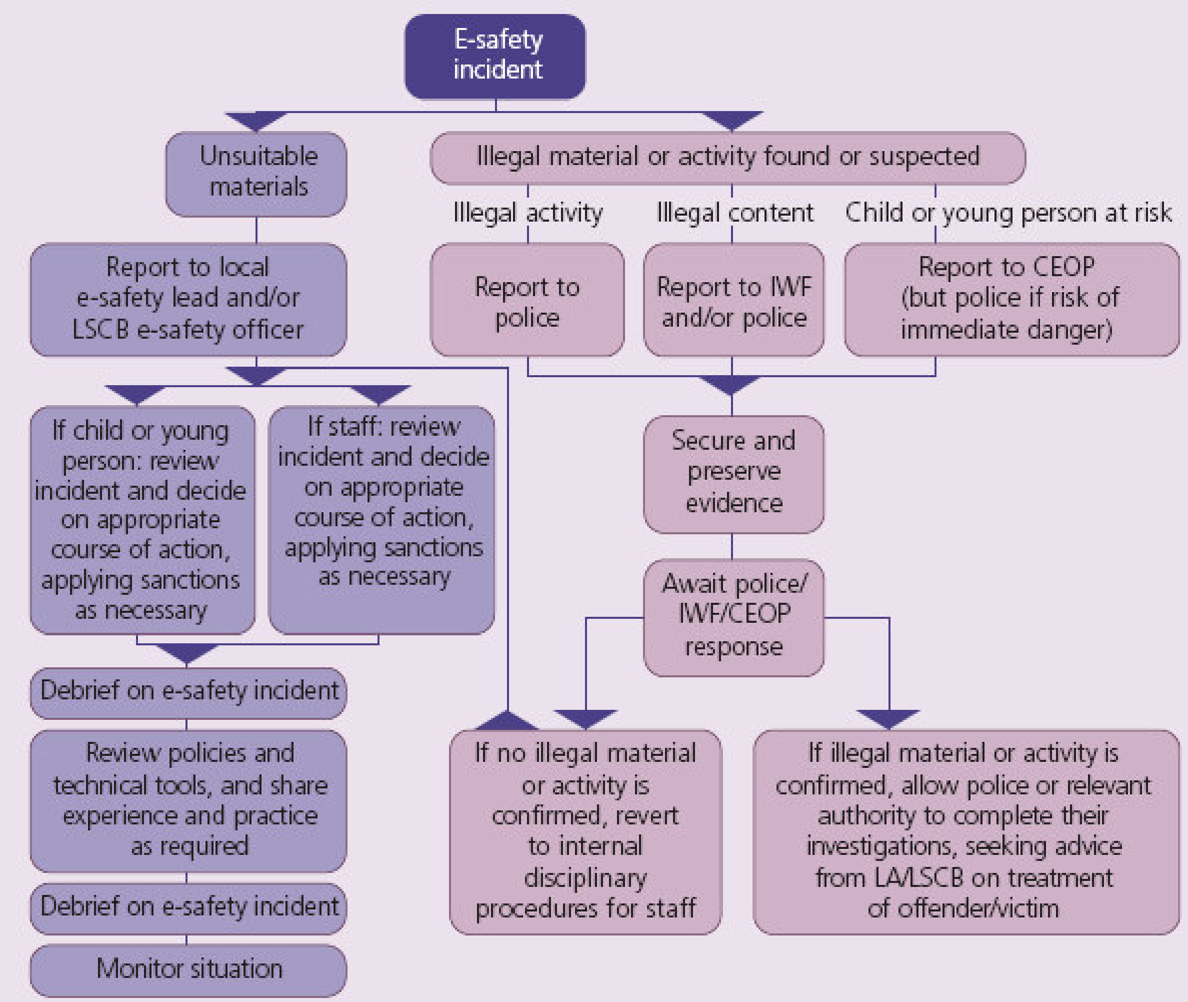
The flowcharts on the next page are adapted from the Northern Grid for Learning and BECTA policies and illustrate the approach to investigating an incident of concern. The response required will depend on the nature of the incident. Concerns may relate to:

- The accidental access to inappropriate material

- The deliberate access to inappropriate material
- Accidental access to illegal material
- Deliberate access to inappropriate material
- Inappropriate or illegal use of technologies
- Bullying or harassment using technology

Flow chart for responding to e-safety incidents

(Reference BECTA: safeguarding children on line: a guide for Local Authorities and LSCB's)


E-safety incident
Unsuitable materials
Illegal material or activity found or suspected
Illegal activity
Illegal content
Child or young person at risk
Report to local e-safety lead and/or LSCB e-safety officer
Report to police
Report to IWF and/or police
Report to CEOP (but police if risk of immediate danger)
If child or young person: review incident and decide on appropriate course of action, applying sanctions as necessary
If staff: review incident and decide on appropriate course of action, applying sanctions as necessary
Secure and preserve evidence
Await police/ IWF/CEOP response
Debrief on e-safety incident
Review policies and technical tools, and share experience and practice as required
Debrief on e-safety incident
Monitor situation
If no illegal material or activity is confirmed, revert to internal disciplinary procedures for staff
If illegal material or activity is confirmed, allow police or relevant authority to complete their investigations, seeking advice from LA/LSCB on treatment of offender/victim

Committing an Illegal Act - Did You Know?

1

Receiving unsolicited emails that may contain potentially illegal material (either as an attachment or in a URL) is not an illegal offence

2

If you receive potentially illegal material you could easily commit an illegal act - **do not open the material or personally investigate**

3

Opening an attachment or URL that proves to hold illegal content **is an illegal act** and is classed as possession of illegal material

4

Showing anyone else illegal material that you have received **is an illegal act**

5

Printing a copy of the offensive email to report it to someone else **is an illegal act** and is classed as producing illegal material

6

Having printed a copy of the material if you give it to someone else **is an illegal act** and is classed as distributing illegal material

7

Within 4 simple steps you could easily break the law 4 times. Each is a serious offence

8

Never open unsolicited URLs or attachments. If you are suspicious that the content could be illegal report it and log that you have received it

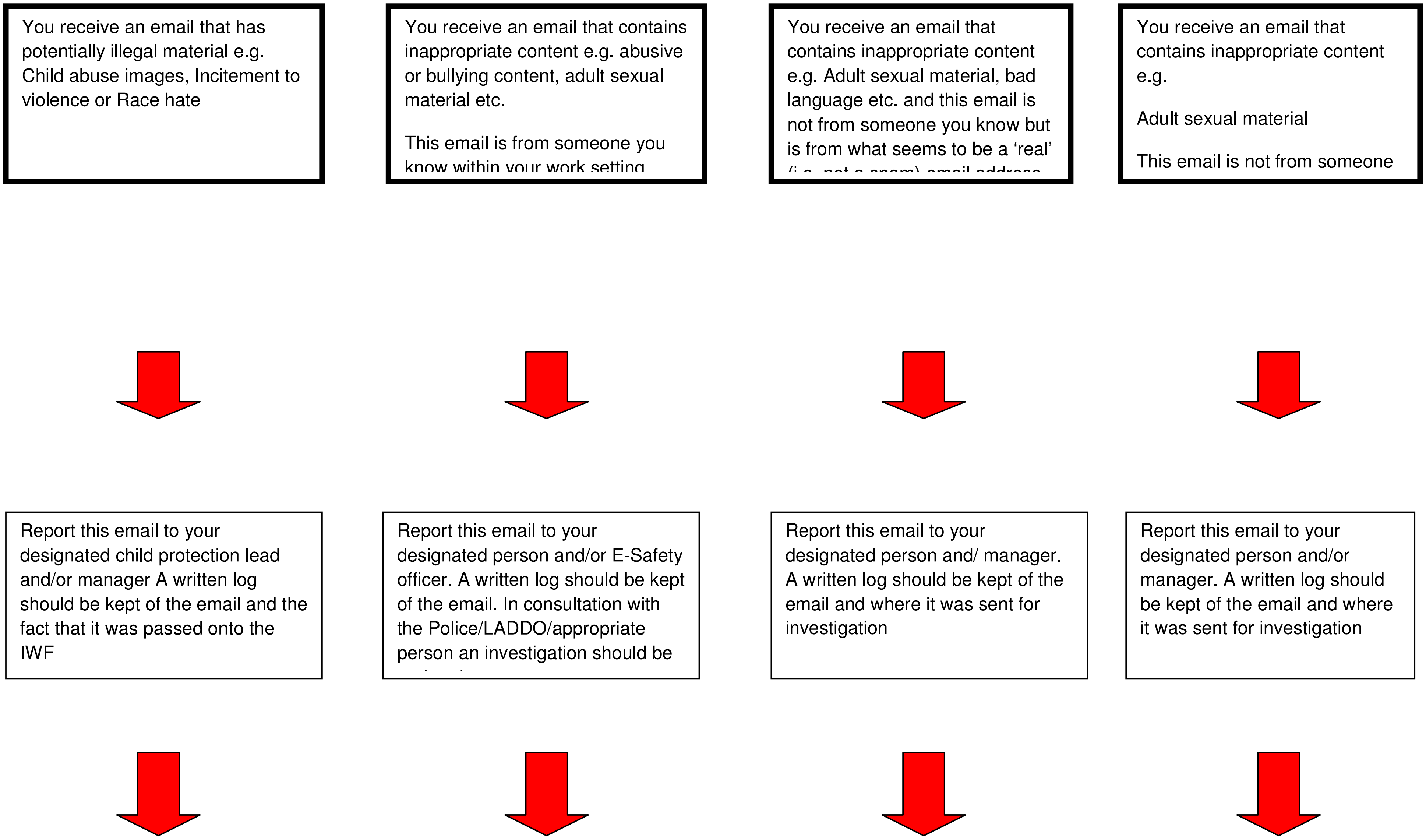
9

Always report potential illegal content to the Internet Watch Foundation at www.iwf.org.uk

They are licensed to investigate **you are**

Never personally investigate. If you open illegal content accidentally report it to your manager and IWF. Go to the IWF website and click on the report button. **Do not copy and paste the URL, write it down and type it into the reporting screen. This prevents accidental opening**. Once the email has been logged and reported to the IWF delete it from your inbox. If you are unsure, contact the IWF for advice on 01223 237 700. **The Internet Watch Foundation only deals with illegal content, please see their website for information and advice. Please note this guidance only relates to illegal content not inappropriate.**

What to do with Suspicious Email received at work



You receive an email that has potentially illegal material e.g. Child abuse images, Incitement to violence or Race hate

Report this email to your designated child protection lead and/or manager A written log should be kept of the email and the fact that it was passed onto the IWF

You receive an email that contains inappropriate content e.g. abusive or bullying content, adult sexual material etc.

This email is from someone you know within your work setting

Report this email to your designated person and/or E-Safety officer. A written log should be kept of the email. In consultation with the Police/LADDO/appropriate person an investigation should be

You receive an email that contains inappropriate content e.g. Adult sexual material, bad language etc. and this email is not from someone you know but is from what seems to be a 'real' (i.e. not a spam) email address

Report this email to your designated person and/ manager. A written log should be kept of the email and where it was sent for investigation

You receive an email that contains inappropriate content e.g.

Adult sexual material

This email is not from someone

Report this email to your designated person and/or manager. A written log should be kept of the email and where it was sent for investigation

Report this email to the IWF

Go to www.iwf.org.uk

Click on the report button and follow the instructions and their

Consider whether Module 12 of the SET Procedures applies – If yes refer to the Local authority Designated Officer

If the sender's ISP is known – can a complaint be realised under their acceptable use policy if appropriate?

Report this to Easynet on abuse@uk.easynet.net

In all cases secure the email in a folder and only delete when the investigation has been completed or you are advised to do so.

In the case of potential illegal material do not show the content of this email to anyone but report it to your manager and take the advice of the Internet Watch Foundation.

Do NOT always presume that the sender's email address is telling you the truth – Spammers can and do fake other's email addresses. If you are unsure how to proceed please contact the Northern Grid for Learning on 0191 4611844

5. Responding to incidents of misuse by those working with children

Even with all the policies and technological solutions in place, there may still be occasions when misuse of the internet and related technologies occur. Organisations must ensure that they have appropriate strategies in place for responding to such instances where this involves those working with children and young people. Responding appropriately to a breach of internet safety can cause some uncertainty, sometimes over what the nature of the offence may be, or even because of a lack of understanding of the potential seriousness of incidents involving ICT. Organisations should have in place policies on acceptable use to advise them in such instances. Where incidents of concern are of a child protection nature, organisations will also need to refer to module 12 of the SET Procedures.

Responding to incidents of misuse by children and young people

Incidents may involve:

1. Sending nuisance text messages
2. The unauthorised taking of images with a mobile phone camera
3. Racially motivated abuse via technology.

Organisational procedures will always need to be consistent with those in the SET Procedures, and the importance of all incidents being documented is important. If the behaviour is repeated, or the misconduct escalates, it can then be responded to more seriously if there is evidence of previous events. With many incidents the importance of providing education for young people is important, for example are people aware that distributing inappropriate images on a mobile phone may be an offence, young people may not be aware of the consequences of their actions.

Incidents involving illegal materials or activities

This may include the viewing, possession, making and distribution of indecent images of children or serious stalking or harassment facilitated by communication technologies. Such criminal offences may be committed by those working with children and children alike.

Indecent images of children are defined under Section 7 of the Protection of Children Act 1978 (as amended by Section 84 of the Criminal Justice and Public Order Act 1994). References to indecent photographs under the Act include:

- Data stored on a computer disk or by other electronic means that is capable of conversion into a photograph.

The Protection from Harassment Act 1997 is intended to prevent 'stalking' and other similar unsocial conduct. It states that a person must not pursue a course of conduct which amounts to harassment of another, and which he/she knows, or ought to know, amounts to harassment of the other. Although the term is deliberately not defined in the Act, words such as ‘alarm’,’ distress’ or ‘torment’ fit the term most accurately, and some adverse impact on the victim is required. To constitute a ‘course of conduct’, harassment must take place on a minimum of two occasions.

How to respond to incidents of misuse

- Discovery of indecent material within an organisations network is a very serious situation, and must always be reported to the police.
- It is important that the material is not downloaded, printed or sent by email, because doing so will be an offence in itself.
- If at all possible, do absolutely nothing to the suspect computer or computers, including turning them on or off. It may be necessary to shut down the whole network, but do not do this unless instructed by the police.
- Ensure that everyone is kept away and that nothing is touched.
- Under no circumstances should your organisation attempt to conduct an investigation of their own, as this may compromise the evidence if a legal case were to result. In some cases this may constitute a criminal offence in itself.

- In cases of staff involvement with indecent materials, seek advice from your HR department ensuring that you follow the procedures in SET module 12 and refer to the LADO where appropriate.

Further information on illegal content – including when, where and how to report it – can also be found on the Internet Watch Foundation website http://www.iwf.org.uk.

Training

All those who come into contact with children will need to develop some e-safety awareness. This may include general e-safety awareness, technical awareness and understanding what to do when a concern is raised.

Monitoring and evaluating of e-safety incidence

Monitoring and reporting of e-safety issues and incidents is very important. Not only will it provide a permanent record of incidents, outcomes and actions taken, it will also provide an important tool for reflecting on and revising practice, and identifying emerging trends which can be addressed before they become problematic.

Questions for organisations to consider in evaluating their effectiveness include:

- Do you have a policy/guidance on e-Safety?
- Do you have an acceptable use policy?
- Do you provide staff training on e-safety?
- Is there an identified e-safety lead in your organisation?
- Are you using an accredited internet service provider?
- Do you ensure the voice and views of children and young people are used to inform policy, guidance and training?
- Do you monitor your policy and identify any trends arising?

Further details of how to assess your organisations effectiveness are included in the best practice check list provided as supplementary materials to this document. The LSCB will also be producing training materials to support organisations in developing e- safety awareness.

Appendix 1

Glossary

Acceptable use: A policy that a user must agree to abide by policy (AUP) in order to gain access to a network or the internet. It may also cover how other communications devices, such as mobile phones and camera phones, can be used on the premises.

Adware: A program that appears to be free but may be paid for by companies whose products are advertised every time you use it. Some adware contains small programs that track the websites you visit on the internet, reporting the information back to marketing sites which then tailor advertisements to your interests. This is similar to spyware. The most sophisticated spyware can even track what keys you are hitting when you type, so using a **firewall** is vital to filter out these kinds of programs.

Avatar: A graphical representation of a person. Avatars are sometimes used in chat and multi-user gaming environments.

Blog: A blog, also known as a weblog, is a form of online diary or journal. Blogs contain short, frequently updated posts, arranged chronologically with the most recently posted item appearing at the top of the page. In addition to text, blogs can contain photos, images, sound, archives and related links, and can incorporate comments from visitors.

Bluetooth: Bluetooth is a telecommunications industry standard which allows mobile phones, computers and PDAs to connect using a short-range wireless connection.

Bookmarking: The process of storing the address of a website or internet document on your computer, so that you can find it again easily.

Chatroom: An area on the internet or other computer network where users can communicate in real time, often about a specific topic. As chat software develops, individuals are not only able to send text messages to chat rooms but, in some instances, also have the ability to communicate through their actual voices (voice chat) via headsets, or indeed, actually be seen by chat room members, through web cams.

When joining a chat service or room an individual must select an onscreen name or nickname, and all members of a chat room are usually listed down one side of the screen. As well as chatting in a specific room, individuals can request and initiate private conversations with other members of a chat room, which can appear similar to instant messaging.

Cookie: a piece of data stored in your computer after you have visited a website, that allows the web page to be down loaded more quickly.

Cyberspace: *Cyberspace* is a metaphor for the environment in which communication over computer networks occurs. The word is often used as an alternative to *internet*.

Digital video: Video captured, manipulated and stored in a digital format.

Filtering: A method used to prevent or block users' access to unsuitable material on the internet.

Firewall: A network security system used to restrict external and internal traffic.

Hacking: The process of illegally breaking into someone else’s computer system breaching the computer’s security.

Internet service provider (ISP): A company providing a connection to the internet and other services, such as browser software, email, a helpline, web space and subscriber-only content.

Instant messaging (IM): Allows users to communicate with other users, providing an easy way of sending short written messages to a few friends online at the same time. It includes text messaging, voice chat, webcams, and file and picture exchange. IM can be a very private form of communication between known friends where the user builds up a list of contacts and is alerted when they are online. IM, however, can also be a public open environment where the user is encouraged to find and make new contacts online.

P2P (peer to peer): The internet is beginning to offer new services alongside websites and chat services, particularly those which enable the swapping and storing of media files (sounds, images and video). This is referred to as *Web 2.0*. These services can enable direct sharing of files – person to person, computer to computer. These services are much harder to moderate than chat rooms and message boards. As ISPs and service operators bring in moderation to make sure their digital services with a social function are safer for children, technology is encouraging social activity away from these safe centres. This means that educating children and young people how to protect themselves online becomes even more important.

Personal digital assistant (PDA): A small, mobile, handheld device that provides computing and information storage/retrieval capabilities, and possibly phone facilities too.

Phishing: When someone tricks you into giving confidential information by asking you to click on a false website and entering your details.

Spam: Unsolicited junk email. The term is also used to describe junk text messages received via mobile phones. A related term, spim (or spIM), describes receiving spam via instant messaging.

SMS: Short messaging service or text messages.

Spoofing: Assuming the identity of someone else, using an email address either guessed or harvested from repositories of valid email addresses (such as the address book of a virus-infected computer). Spoofing is typically practised to veil the source of virus-laden emails or, often, to obtain sensitive information from spam recipients, without revealing the source of the spammer.

Trojan horses: A virus which infects a computer by masquerading as a normal program. The program contains additional features added with malicious intent.

Trojan horses have been known to activate webcams, for example, without the knowledge of the PC user.

Usenet: The part of the internet where **newsgroups** are found.

Video conferencing: The process of conducting a conference between two or more participants over a network, involving audio and often text as well as video.

Vlog: A **blog** which showcases video.

Virus: A computer program which enters a computer, often via email, and carries out a malicious act. A virus in a computer can corrupt or wipe all information in the hard drive, including the system software. All users are advised to guard against this by installing anti-virus software.

WAP: A website designed to be accessed on a small screen like a mobile phone.

Webcam: A webcam is a camera connected to a computer that is connected to the internet. A live picture is uploaded to a website from the camera at regular intervals, typically every few minutes. By looking at the website you can see what the camera sees – almost as it happens.

Weblog: See the entry for ‘blog’ above.

WIFI: Short for wireless fidelity, it is a way of connecting a computer to the internet using radio frequency, rather than cables. A hotspot is where you can access a WIFI network.

Appendix 2

Notes on the legal framework

This section is designed to inform users of legal issues relevant to the use of communications. Many people use the Internet regularly without being aware that some of the activities they take part in are potentially illegal.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.

Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.

It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment.

This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Data Protection Act 1998

“Organisations have a right (and in the case of providing services to children, a duty) to monitor use of their technical infrastructures to prevent them being used inappropriately, for unlawful purposes or to distribute offensive material.

However, an individual also has a right to privacy. It is the duty of any organisation that provides online access to balance these two separate rights and, in the case of children’s and community services different policies may be needed for children and adults within these settings.

In any case, organisations should be open on the subject of monitoring the use of their technical networks, and this can typically be achieved through the acceptable use policy, as previously discussed.” (BECTA)

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual’s motivation, the Act makes it a criminal offence to:

- Gain access to computer files or software without permission (for example using someone else’s password to access files);
- Gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or
- Impair the operation of a computer or program (for example caused by viruses or denial of service attacks).

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her “work” without permission.

The material to which copyright may attach (known in the business as “work”) must be the author’s own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.

It is an infringement of copyright to copy all or a substantial part of anyone’s work without obtaining the author’s permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else’s material.

It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Regulation of Investigatory Powers Act 2000

“The Regulation of Investigatory Powers Act (RIPA) provides the legal framework for using methods of surveillance and information gathering to help the prevention of crime. It includes, among other provisions, the interception of communications, the acquisition and disclosure of data relating to communications, and access to electronic data protected by encryption or passwords.

Each police force and most councils are defined as a ‘public authority’ to which RIPA applies. The forms of surveillance that the police and any council are entitled to authorise are covert directed surveillance and the use of covert human intelligence sources (informants). In any council, only officers of the rank of deputy chief officer and above may be designated as authorising officers under RIPA. No covert directed surveillance or use of covert human intelligence sources may be undertaken without obtaining authority from such an authorising officer.

RIPA requires that third parties that are required to provide information about other people subject to surveillance and investigation should be approached for that information in a highly controlled manner by means of standard forms published by the Home Office.

It is possible that, in their role of safeguarding children, LSCBs and member agencies may be subject to the provisions of RIPA. As such, they should be aware of the appropriate response if such a request is made.” (Ref: BECTA 2007)

The Telecommunications (Lawful Business Practice) (Interception of Communications)

Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored.

Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

(Ref Kent schools e-safety policy 2007)

Internet use and abuse is governed by many civil or criminal laws in the UK. While this list is not exhaustive, some of the key provisions are summarised below:

- Computer Misuse Act 1990 (including hacking, denial of service attacks) http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm

- Copyright, Designs and Patents Act 1988(including copyright theft) http://www.opsi.gov.uk/acts/acts1988/Ukpga_19880048_en_1.htm

- Crime and Disorder Act 1998 http://www.opsi.gov.uk/acts/acts1998/19980037.htm

- Data Protection Act 1998 http://www.opsi.gov.uk/acts/acts1998/19980029.htm

- Privacy and Electronic Communications (EC Directive) Regulations 2003(including spam) http://www.opsi.gov.uk/si/si2003/20032426.htm

- Protection from Harassment Act 1997 (including harassment, bullying, and cyber stalking) http://www.opsi.gov.uk/acts/acts1997/1997040.htm

- Protection of Children Act 1978, as amended by Section 84 of the Criminal Justice and Public Order Act 1994 (including indecent images of children) http://www.opsi.gov.uk/acts/acts1994/Ukpga_19940033_en_1.htm

- Malicious Communications Act 1988 (including harassment, bullying, and cyber stalking) http://www.opsi.gov.uk/acts/acts1988/Ukpga_19880027_en_1.htm

- Sexual Offences Act 2003 (including grooming) http://www.opsi.gov.uk/acts/acts2003/20030042.htm

- The Obscene Publications Act 1959 and 1964 (including illegal material on, or transmitted via, the web and electronic communications) - not available online

- The Telecommunications Act 1984 (including illegal material on, or transmitted via, the web and electronic communications) - Not available online

Appendix 3

Sources of external e-safety support

There are a number of agencies that can provide help either in terms of providing training on e-safety issues, responding to specific e-safety incidents, or supporting the key stakeholders in a child life. Some of these are described briefly below.

Child Exploitation and Online Protection Centre

[http://www.ceop.gov.uk]

The Child Exploitation and Online Protection (CEOP) Centre aims to tackle child sex abuse wherever and whenever it happens. Part of their strategy for achieving this is to provide internet safety advice for parents and carers, training for educators and child protection professionals, and providing a 'virtual police station' for reporting abuse on the internet.

Some of these services are outlined briefly below.

Thinkuknow – online safety for young people and their parents

[http://www.thinkuknow.co.uk]

The CEOP Thinkuknow website provides a range of information on online safety for young people, with key topics including mobiles, gaming, social networking, chatting, podcasts, blogs, and peer-to-peer TV.

The content of the site is based around three key messages:

- How to have fun online
- How to stay in control online
- How to report online.

A section of the website is aimed specifically at parents and carers to try to help them understand more about what their child may be doing online.

The site also provides a prominent link to the CEOP report abuse service for reporting suspicious behaviour online with or towards a child (see below).

Training for educators

[http://www.thinkuknow.co.uk/teachers]

CEOP offers training to educational professionals through the Thinkuknow Education Programme, aimed at children aged 11-16.

Once trained, educators are able to directly deliver the Thinkuknow programme to children. Further completion of the CEOP Ambassador Training scheme will also allow educators to cascade the training to colleagues.

Training for child protection professionals

[http://www.ceop.gov.uk/training/courses.html]

CEOP work alongside colleagues in the criminal justice and child protection agencies in the UK and abroad to add value to existing services and provide greater support to professionals working in this area.

They provide a series of specialist training courses aimed at professionals who:

- conduct criminal investigations where the sexual abuse of children is a factor
- manage offenders in the community or within the justice system
- take responsibility for safeguarding children from sexual predators.

The training courses are designed to help delegates better understand the nature of sexual offending and to develop the skills and knowledge that can better equip professionals to deal with the very difficult and distressing nature of such crimes. One of the courses deals specifically with internet sex offenders.

Reporting abuse

CEOP provides a facility, in association with the Virtual Global Taskforce, to report any inappropriate or potentially illegal activity towards a child online. This might be an online conversation with someone who a child thinks may be an adult, who is treating a child in a way which makes them feel uncomfortable, or who is trying to meet a child for sex.

If a child is in immediate danger, dial 999 for immediate police assistance.

There are prominent reporting links from the CEOP website, the Virtual Global Taskforce website and the Thinkuknow website. A reporting link is also available as a tab option on other sites

Virtual Global Taskforce

[http://www.virtualglobaltaskforce.com]

The Virtual Global Taskforce (VGT) is made up of law enforcement agencies from around the world working together to fight child abuse online. The aim of the VGT is to build an effective, international partnership of law enforcement agencies that helps to protect children from online child abuse.

A section for young people provides links to a range of useful resources, and the site also provides a direct link for reporting abuse.

Internet Watch Foundation

[http://www.iwf.org.uk]

The Internet Watch Foundation (IWF) is the UK hotline for reporting illegal content, specifically child abuse images hosted worldwide and content that is criminally obscene and incitement to racial hatred, hosted in the UK. A prominent link for reporting illegal content is available from the homepage of the IWF website.

The IWF website also provides an overview of the IWF URL list of online child abuse content, which should be included as an absolute minimum in internet filtering services

NSPCC and related services

[http://www.nspcc.org.uk]

ChildLine

[http://www.childline.org.uk]

NSPCC services include ChildLine, a free and confidential helpline for children in danger and distress. Children and young people in the UK can call 0800 1111 to talk about any problem, 24 hours a day.

There4me.com

There4me.com is an online advice and information service specifically aimed at children aged 12 – 16, covering topics such as internet safety, abuse and bullying. Services include message boards, a private online in-box, and 'real time' one-to-one counselling with NSPCC advisers.

Child Protection Helpline

The NSPCC Child Protection Helpline offers advice and support to anyone concerned about the welfare of a child. The helpline is a free, confidential service open 24 hours a day, seven days a week on 0808 800 5000

Stop it Now!

[http://www.stopitnow.org.uk]

Stop it Now! aims to prevent child sexual abuse by increasing public awareness and empowering people to act responsibly to protect children.

Stop it Now! operates a freephone helpline on 0808 1000 900. It offers confidential advice and support to adults that might be unsure or worried about their own thoughts or behaviour towards children, or the behaviour of someone they know, whether they are an adult or a child.

Experienced advisors are available to discuss concerns and can offer confidential advice and guidance on an appropriate course of action.

(Adapted from BECTA: safeguarding children in a digital world: Developing an LSCB e-safety strategy)

Bullying online

http://www.bullying.co.uk

Bullying Online is an online help and advice service combating all forms of bullying. Recognising that many young people that have lost friends through being bullied in the real world may turn to the internet to make new friends, the ‘Staying safe in cyberspace’ section gives tips for staying safe in chat rooms. There is also a section on mobile phone bullying, giving tips on how to protect yourself, and information on how the law can help. The site provides information for pupils, teachers and parents.

Parentscentre

http://www.parentscentre.gov.uk

Parentscentre offers support, information and advice on children’s learning and the education system, including use of the internet.

Acknowledgments

This document draws upon existing good practice and guidance provided by:

BECTA:

Becta e-safety resources online
[http://www.becta.org.uk]

The Becta website aims to highlight e-safety issues relating to new technologies, and provide practical information and advice for schools, local authorities and LSCBs on how to use these technologies safely.

BECTA (2007) Safeguarding children online: a check list for Local Authorities and Local Safeguarding Children Boards

BECTA (2008) Safeguarding Children in a digital world

CEOP www.ceop.org.uk

Kent: e-safety policy   www.clusterweb.org.uk

Section 2 - Developing an E-Safety Policy

BEST PRACTICE CHECKLIST

This checklist has been developed from “Safeguarding Children on line - a checklist for local authorities and LSCB’s” BECTA. When completed it aims to give LSCB partners a snapshot of their e-safety issues and risks and to sign post activities that they need to develop across services. It is recommended for use in schools, youth centres, libraries and any services where children have access to technology and should be read in conjunction with the LSCB guidance on developing an e-safety policy.

The terms ‘e-safety’ or ‘online’, refers to all fixed and mobile technologies which children and young people might encounter, now and in the future, which allow them access to content and communications that could raise issues or pose risks to their wellbeing and safety.

Policies and practices

In any context, effective policy is the backbone of good practice, and organisations should consider developing comprehensive and coherent e-safety policies for all services within their remit.

	In place y/n	Evidence attached	Areas for development

	In place y/n	Evidence attached	Areas for development
Does the organisation have an e-safety policy?			
Who is responsible for co-ordinating e-safety in the organisation to ensure that best practice is developed, implemented and kept up to date?			
Is there a regular risk assessment of your e-safety infrastructure?			
Do all services have acceptable use polices (AUP's) of ICT by children, young people and staff? Have staff signed an acceptable use policy? *Is the application of these policies monitored?* *Are the AUPs kept up to date in line with changing issues and technologies?*			
Are the children and young people that use your services aware of their responsibilities for staying safe when online?			

	In place y/n	Evidence attached	Areas for development
Are they aware of their responsibilities to others? Do they know who to speak to if they encounter problems online or accidentally access inappropriate materials? *Consider links to “thinkuknow” website as a means of reporting*			
Is the privacy of children and young people protected when they are online? *e.g. if you include photographs of children on your website, for example, you will need to gain permission from the parents or guardian to use those images*.			
What are the procedures for reporting e-safety incidents of misuse? Are staff aware of their responsibilities in responding to certain types of incident?			

	In place y/n	Evidence attached	Areas for development
How are incidents escalated? *Do you pass information to the Internet Watch foundation?*			

Infrastructure and technology

	In place y/n	Evidence attached	Areas for development
Are there minimum standards for technical e-safety in all settings where children may access ICT? *Do you have filtering systems in place to prevent access to inappropriate material?* *Are you using accredited ISPs?* *Becta's functional and technical specifications give further information.* *[**http://www.becta.org.uk/industry/techstandards**].*			
How are technical standards monitored? *Are local issues centrally reviewed for evidence of emerging problems or trends?*			

Communication and Training

	In place y/n	Evidence attached	Areas for development
How does your organisation seek to 'raise awareness about the safe use of the internet' – and other technologies?			

	In place y/n	Evidence attached	Areas for development
a)with children and young people b)with staff c)parents and carers			
Who co-ordinates activities in the 'development and delivery of training and education programm with CEOP'?			
What is the organisations strategy for educating and training staff in e-safety? Have your staff received e-safety awareness training? *This should include induction of new staff, plus ongoing support and supervision of existing staff. Staff should be aware of appropriate local, regional and national issues with regard to e-safety, and should be confident in their abilities to escalate an incident as necessary and appropriate.*			
Is existing good practice within Essex shared? *Many organisations may*			

	In place y/n	Evidence attached	Areas for development
already have e-safety strategies in place. If you are interested in sharing your good practice, please send any materials to the ESCB who will share these across other services.			
How are children with additional vulnerabilities safeguarded on line? *e.g: children and young people outside of mainstream education, children with disabilities*			
How will the impact of education and training be monitored and evaluated?			
What e-safety information and guidance is provided to parents and carers?	]		

Standards and inspection

	In place Y/N	Evidence attached	Areas for development
Who is responsible for monitoring e-safety measures? *As discussed in the policies and practices section, a responsible officer should take the lead in developing an e-safety agenda.*			
How is activity monitoring co-ordinated, particularly where several agencies have responsibility in this area? *Co-ordination is essential in order to incorporate recommendations and guidance from all agencies involved in child protection into local e-safety policies and practices*. Are emerging themes and trends passed to a central coordinator with you organisation?			
How is performance measured, and how is progress benchmarked? How is good practice shared?			

How is poor performance managed? Who drives forward recommendations?			

Section 3 - Safeguarding Your Organisation – Your Organisation's Use of Social Media

Introduction

Interactive social media technology has revolutionised the way people connect and interact. Facebook, Twitter, Flickr, blogs, instant messaging and photo and video exchange sites are increasingly popular, and provide an opportunity to connect with children, young people and vulnerable adults.

However the use of social networking sites also brings with it a range of potential safeguarding risks to children, young people and vulnerable adults.

This paper aims to provide you with advice and guidance about how you can make the most of networking sites, while safeguarding children, young people and vulnerable adults.

What is Social Media?

Social media refers to the latest generation of interactive online services such as blogs, discussion forums, pod casts and instant messaging.

Social media includes:

- collaborative projects (for example, Wikipedia)
- social networking sites e.g. Bebo, Facebook, Piczo, Hi5 and MySpace
- blogs and micro-blogging services e.g. Twitter
- content sharing e.g. video-sharing services e.g. YouTube or photo-sharing services e.g. Flickr
- online games and virtual reality e.g. Second Life

Social media is a dynamic, constantly-evolving form of communication that allows people to take part in online communities, generate content and share information with others. Users can now access interactive services across a multitude of services and devices, such as mobile phones, personal digital assistants (PDAs), game consoles and personal computers.

Social media services are particularly popular with children and young people as they offer them opportunities to be creative, connect with people all over the world and share interests. Young people can design their own personal webpage, interact with friends through instant messaging and chat rooms, upload and share images and videos, create blogs, publish and share music and create or join wider communities or interest groups in areas such as music or sports etc.

Benefits of Social Media

Social media provides a range of unique opportunities for organisations. It can help organisations:

- promote the benefits of their services to all children, young people and vulnerable adults and it can be a route to the hard-to-reach groups too
- engage, connect and develop unique interaction with people in a creative and dynamic medium where users are active participants
- disseminate messages about events or campaigns virally among supporters in online communities

It is important for organisations to give careful consideration to the use of social media and to balance the benefits of creativity, spontaneity and immediacy of the communication with the potential risks, including the risks to children, young people and vulnerable adults.

You should only move forward with developing social networking sites when safeguarding issues have been adequately assessed and addressed to minimise these potential risks.

Risks with Social Networking sites

With all emerging technologies there is also the potential for misuse. Risks associated with user interactive services include: cyber bullying, grooming and potential abuse, online predators, identity theft and exposure to inappropriate content, including self-harm, racism, hate and adult pornography. Most children, young people and vulnerable adults use the internet positively, but sometimes behave in ways that may place themselves at risk. Some risks do not necessarily arise from the technology itself but result from offline behaviours that are extended into the online world, and vice versa.

Potential risks can include, but are not limited to:

- bullying by peers and people they consider 'friends'
- posting personal information that can identify and locate a child, young people and vulnerable adults offline
- sexual grooming, luring, exploitation and abuse contact with strangers

- exposure to inappropriate content
- involvement in making or distributing illegal or inappropriate content
- theft of personal information
- exposure to information and interaction with others who encourage self harm
- exposure to racist or hate material
- encouragement of violent behaviour, such as 'happy slapping'
- glorifying activities such as drug taking or excessive drinking
- physical harm to people in making video content, such as enacting and imitating stunts and risk taking activities, leaving and running away from home as a result of contacts made online.

Setting up a Social Network Service

a) *Your organisation should follow relevant legislation and good practice guidance when engaging with social media companies.*

Depending upon the size of your organisation, you may wish to engage with a specialist social media company. These companies help brands analyse the market, optimise your audience, keep your content online fresh and moderate your webpage/ profile.

Some companies collect and use data for online advertising purposes. This is a growing practice known as online behavioural advertising and involves the delivery of relevant advertising to groups of anonymous web users, based upon previous internet browsing activity.

Recent good practice guidance produced by the social media industry (Internet Advertising Bureau) recommends that companies should not create or sell online behavioural segments intended for the sole purpose of targeting children they know to be under 13yrs.The guidance also sets out core commitments about providing notice, giving choice and educating consumers about how data will be collected. Personally identifiable information which is data that, by themselves or in conjunction with other data held uniquely identifies an individual offline is also covered.

Social media and moderation companies may also offer to moderate your webpage/profile on your behalf. This involves assigning a person to moderate or manage the interaction with users on the webpage/profile. This person, sometimes referred to as a moderator, is most likely to have online contact with younger users interacting with the webpage/profile. You should ensure that this person is CRB checked as part as safe recruitment process. If the company is based outside of the UK i.e. based in the US, ask if they have equivalent legislation/guidelines or if they follow the principles of UK law and guidance.

b) *Get to know the service you want to provide*

Once you've identified the service you want to use (e.g. Facebook), make sure you're up to speed with the way this service operates, and the potential safeguarding implications for children, young people, vulnerable adults and staff before setting up your presence.

Specifically, you should look at privacy and safety tools, the terms of service (these will usually cover acceptable and unacceptable behaviour), and how users can contact the service if they have a concern or complaint.

Also does the organisation adhere to relevant legislation and good practice guidelines. In the UK this includes:

- Home Office Task Force on Child Protection and the Internet: good practice guidelines on Chat, Instant Messaging, Web Based Services, Moderation, Safe Search and Social Networking Services and other user interactive services.
- Collection and use of personal data and the Data Protection Act 1998.
- Having safe recruitment processes for moderators of social networking site that involve children and young people.
- If the company is based outside of the UK e.g. based in the US, ask if they have equivalent legislation/guidelines or if they follow the principles of UK law and guidance.

When contracting or outsourcing this work ask to see the organisation’s safety and privacy policy which could include: safety tools in place; safe use guidelines and complaints reporting procedures; relevant criminal record checking procedures for moderators; and adherence to relevant legal or good practice guidance

c) *Decide who will manage your social media*

Decide who will be responsible for setting up, managing and moderating (overseeing / reviewing /responding to posted content) your web page or profile. This person will oversee the content that will appear, will decide which links to other sites to accept, and will have online contact with the children, young people and vulnerable adults who interact with your webpage or profile. Ensure they understand online safeguarding issues, including warning signs of grooming and sexual exploitation and they have an enhanced CRB check.

d) *Don't target underage children*

Social networking services usually have a minimum requirement age of 13

e) *Avoid taking personal details of children and young people*

Don't ask users to divulge any personal details - including home and email addresses, schools or mobile numbers

f) *Be careful how you use images of children, young people and vulnerable adults*

Photographs and videos of children, young people and vulnerable adults on websites can be used to identify them and make them vulnerable to people who wish to groom them for abuse. To counteract this risk, Southend Safeguarding Children Board use of images guidance must be considered before any images are used on websites.

- consider using models or illustrations to promote an activity
- if a child or vulnerable adult is named, do not use their image
- if an image is used, do not name the child or vulnerable adult
- obtain parents' written consent to use photographs on web sites

Images showing children and young people under the age of 18 and vulnerable adults should not be used on any organisations social networking site e.g. Facebook, Flickr, Twitter due to the potential for:

- the tagging of children and young people and vulnerable adults thus identifying them at a location and allowing the opportunity for abusers to identify and locate them on social networking sites
- the morphing of the image
- personal intimidation by posting derogatory, abusive and threatening comments
- cyber bullying

For the above reasons and the potential to post images of bullying and other inappropriate live incidents that occur offline, there should not be the ability for users to upload their own images on an organisation's website or social networking site.

g) *Ensure that staff and volunteers are aware of the need to protect their privacy online and the organisation's approach to use of social networking sites*

Make sure that staff and volunteers are aware of the need to protect their own privacy online. They should understand the risks in posting and sharing content which may damage their reputation before they link their webpage/profile to the sports profile.

h) *Ensure that online safeguarding issues are fully integrated into your existing safeguarding strategy, policies and procedures and training*

All staff and volunteers who use the social networking site should be familiar with how to identify abuse online and their organisation's reporting procedures if they are concerned about online abuse which should include the reporting of potentially illegal/abusive content or activity, including child sexual abusive images and online grooming.

As a reminder in the UK, you should report illegal sexual child abuse images to the Internet Watch Foundation at www.iwf.org .Reports about suspicious behaviour towards children and young people in an online environment should be made to the Child Exploitation and Online Protection Centre (CEOP) at www.ceop.uk.

Also remember that where a child, young person or vulnerable adult may be in immediate danger, individuals should always dial 999 for police assistance.

i) *The site should provide links to safety and support organisations on the profile, or better still accept these organisations as 'Friends' so that they appear on the sport webpage/profile in the 'Friends' section.*

These will include CEOP and the Internet Watch Foundation (as above) but other organisations include;

- For safety and education materials www.thinkuknow.co.uk
- For resources aimed to help educate young people, parents, teachers and volunteers about safe and positive use of the internet **- Childnet International**: www.childnet-int.org
- For a service provided by the NSPCC offering a free and confidential helpline for children in danger and distress – Childline www.childline.org.uk 0800 1111

Acknowledgements

This document is mainly based on sections of the Dudley Safeguarding Children Board and Dudley Safeguarding Vulnerable Adults Board document 'Social networking services & social media**:** Guidelines for safeguarding children, young people and vulnerable adults 2011

Other acknowledgements include;

- NSPCC Child Protection in Sport Unit Briefings

Social Networking services, social media and sport: Guidelines for safeguarding children and young people

- Home Office Task Force on Child Protection on the Internet

Good practice guidance for the providers of social networking and other user interactive services 2008

Sources of Information

Byron Review

The Government commissioned the Byron Review to look into internet-related risks for children. The result is the report: 'Safer Children in a Digital World'.
www.dcsf.cov.uk/bvronreview/

Child Exploitation and Online Protection Centre (CEOP)

The CEOP is a police organisation concerned with the protection of children and young people from sexual abuse and exploitation, with a particular focus on the online environment. It also runs an education programme called 'Thinkuknow' for professionals to use with children and young people to help keep them safe online.

In association with the Virtual Global Taskforce, an international group of agencies that tackle abuse, CEOP provides an online facility for people to report sexually inappropriate or potentially illegal online activity towards a child or young person. This might include an adult who is engaging a child in an online conversation in a way that makes the child feel sexually uncomfortable, exposing a child to illegal or pornographic material, or trying to meet a child for sexual purposes.

Where a child or young person may be in immediate danger, always dial 999 for police assistance.

www.ceop.gov.uk www.thinkuknow.co.uk

Childnet International

Childnet International is a charity that is helping to make the internet a safe place for children. It has developed a set of award-winning resources called 'Know IT' All that aim to educate young people, parents, teachers and volunteers about safe and positive use of the internet. **www.childnet.org.uk**

ChildLine

ChildLine is a service provided by the NSPCC that offers a free, confidential helpline for children in danger and distress. Children and young people in the UK may call 0800 1111 to talk about any problem, 24 hours a day. The Child Line service is delivered in Scotland by Children 1st on behalf of the NSPCC.

www.childline.org.uk

Data Protection and the Information Commission Office

The Information Commissioner's Office has a range of information and guidance on people's rights, responsibilities and obligations related to data protection.' Keeping your personal information personal' is a guide for young people on looking after their personal information on social networking sites.

http://www.ico.gov.uk/Youth/section2/intro.aspx

Social networking services & social media:

Guidelines for safeguarding children, young people and vulnerable adults 2011

24

'Collecting personal information from web sites' is a guide to collecting information online. It includes a section on collecting information about children, publishing information about children and parental consent.

http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/collecting_personal_information_from_websites_v1.0.pdf

www.ico.gov.uk

EU Kids Online project

The EU Kids Online project (2006-2009) examines children's safe use of the internet across 21 countries.

www.lse.ac.uk/collections/EUkidsOnline

Home Office Taskforce on Child Protection on the Internet

The Home Office Taskforce on Child Protection on the Internet is an authoritative source of information on helping children stay safe online.

Social Networking Guidance

http://police.homeoffice.gov.uk/poublications/operational-policing/social-networking-guidance/

Guidance for the Moderation of Interactive Services for Children

http://police.homeoffice.aov.uk/publications/operational-policing/moderation-document-final.pdf

http://police.homeoffice.gov.uk/operational-policing/crime-disorder/child-protection-taskforce

Good Practice Models and Guidance for the Internet Industry on Chat Services, Instant Messaging and Web-based Services

http://police.homeoffice.gov.uk/publications/operational-policing/ho¬_model.pdf

The Internet Advertising Bureau

The Internet Advertising Bureau has guidelines on online advertising.

www.iabuk.net

Cyberbullying

The Teachernet site has a wealth of information on cyberbullying.

www.teachernet.aov.uk/wholeschool/behaviour/tacklinabullvina/cvberbullvina/

Internet Watch Foundation

The Internet Watch Foundation (IWF) is the UK internet hotline for reporting illegal online content specifically child sexual abuse images hosted worldwide and criminally obscene and incitement to racial hatred content which is hosted in the UK. The IWF works in partnership with the online industry, the

Government, law enforcement agencies and other hotlines abroad to remove such content from the internet. A prominent link for reporting illegal content appears on the home page of the IWF website.

www.iwf.ora.uk

Teachtoday

'Teachtoday' provides resources for teachers on the responsible and safe use of new and existing communications technologies. It aims to help schools:

• understand new mobile and internet technologies, including social networking

• know what action to take when facing problems

• find resources to support the teaching of positive, responsible and safe use of technology

www.teachtodav.eu

Section 4 - Personal Use of Social Media

Guidance for organisations on the personal use of social media for adults involved in working for or volunteering with services for children, young people and vulnerable adults

Introduction

Due to the increasing personal use of social media including social networking sites, staff and volunteers working with children, young people and vulnerable adults need to be aware of the impact of their personal use upon their professional/voluntary position.

Organisations may want to offer staff and volunteers guidance to assist them in their personal use of social media to minimise any impact on their professional/volunteering role.

The following suggested guidance, is intended to help safeguard adults from allegations and protect an individual's privacy as well as safeguard vulnerable groups. However each organisation will want to adapt these for their purposes.

Organisations will have to determine the consequences for any failure to comply with the guidelines e.g. it could lead to them taking disciplinary action.

What is Social Media?

Social media refers to the latest generation of interactive online services such as blogs, discussion forums, pod casts and instant messaging.

Social media includes:

- collaborative projects (for example, Wikipedia)

- social networking sites e.g. Bebo, Facebook, Piczo, Hi5 and MySpace

- blogs and micro-blogging services e.g. Twitter

• Content sharing e.g. video-sharing services e.g. YouTube or photo-sharing services e.g. Flickr

• online games and virtual reality e.g. Second Life

Social media is a dynamic, constantly-evolving form of communication that allows people to take part in online communities, generate content and share information with others. Users can now   access interactive services across a multitude of services and devices, such as mobile phones, personal digital assistants (PDAs), game consoles and personal computers.

Social media services are particularly popular with children and young people as they offer them opportunities to be creative, connect with people all over the world and share interests. Young people can design their own personal webpage, interact with friends through instant messaging and chat rooms, upload and share images and videos, create blogs, publish and share music and create or join wider communities or interest groups in areas such as music or sports etc.

Personal use by Staff and Volunteers

In using social media it is essential that adults are safeguarded from allegations, that individual's privacy is protected and that vulnerable groups are safeguarded.

In practice, anything posted on the internet will be there forever and is no longer in the person's control.

Remember when something is on the internet even if it is removed, it may have already been "snapshotted" by a "web crawler" and so will always be there. Current and future employers and service users may see this.

The following are proposed guidelines for staff and volunteers when using social media and in particular social networking sites

a) *Staff and volunteers should keep all professional work completely separate from their private life.*

- Staff and volunteers should have a neutral picture of themselves as their profile image

- Staff and volunteers should not use their personal or professional details (email or telephone) as part of their profile

- Staff and volunteers should not use their personal profiles in any way for official business. If they are going to be a friend of an organisation's official social networking group they need to ensure they have a separate professional profile.

- Staff and volunteers should not make statements or offer advice to others in any official capacity on their personal sites e.g. as Social Worker for Southend Borough Council I suggest that you….

- Staff and volunteers should not refer directly or indirectly to service users or to any other confidential work related information on personal sites

- Staff and volunteers should not post embarrassing material or comments that may call into question their employment status

- Staff and volunteers should not say or do something on social networking sites that brings their organisation into disrepute

b) Children, Young People and Service Users

- Staff and volunteers should not make friendship requests to service users or their families

- Staff and volunteers should not accept friendship requests on social networking or messaging sites from students, pupils, young people (or their parents) or service users that they work with

- Staff and volunteers should not accept friendship requests on social networking or messaging sites from ex pupils or ex service users (or their families) that they have worked with

- If staff or volunteers have younger friends or family members on their social networking groups who are friends with students, pupils, young people (or their parents) or service users that they currently or have worked with, they need to be aware that posts they write will be visible to them

c) Privacy and photographs

- Social networking sites such as Facebook have a range of privacy settings which are often setup to ‘expose’ details to anyone. When ‘open’ anyone can find them from a search of the social networking site or even from a Google search. Therefore, it is important to change settings to ‘just friends’ so that details, comments, photographs can only be seen by invited friends

- Staff and volunteers should not accept friendship requests unless they know the person or want to accept them – they should be prepared for being bombarded with friendship requests from people they do not know

- Staff and volunteers should choose their social networking friends carefully and ask about their privacy controls

- Staff and volunteers should exercise caution. For example, if they write on a friend’s ‘wall’ on Facebook, all of their friends can see their comment even if they are not their friend

- There is a separate privacy setting for Facebook groups and networks. Individuals may have their own profile set to private, however, when joining a group or a network individuals need to be aware that everyone in that group or network is able to see their profile

- If an individual or their friend is tagged in an online photo album (Facebook, Flickr) the whole photo album may be visible to their friends and anyone else tagged in the photo album

- Staff and volunteers should not have to be friends with anyone to be tagged in their photo album, if they are tagged in a photo they can remove the tag but not the photo

- Staff and volunteers should be aware of the privacy settings on photo sharing websites

- Staff and volunteers should be aware that their friends may take and post photos that they may not be happy about. They need to speak to their friend first to request that it is removed rather than contacting the web provider. If they are over the age of 18, the website will only look into issues that contravene their terms and conditions

If the member of staff or volunteer has difficulty in implementing any of this guidance then they must raise this with their line manager and contact their safeguarding lead.

If a member of staff or volunteer has serious complaints about their organisation that they believe are not being addressed then they should use their appropriate whistle blowing procedures

Reporting concerns about possible online abuse

All staff and volunteers should be familiar with their organisation's reporting procedures which should include the reporting of potentially illegal/abusive content or activity, including child sexual abusive images and online grooming. However if the concern is raised in their personal capacity then they should be aware that they need to immediately report online concerns to the Child Exploitation and Online Protection Centre (CEOP) or the police. Law enforcement agencies and the service provider may need to take urgent steps to locate the child and/or remove the content from the internet.

In the UK, they should report illegal sexual child abuse images to the Internet Watch Foundation at www.iwf.org.

Reports about suspicious behaviour towards children and young people in an online environment should be made to the Child Exploitation and Online Protection Centre at www.ceop.uk.

Where a child, young person or vulnerable adult may be in immediate danger, individuals should always dial 999 for police assistance.

Acknowledgements

This document is mainly based on sections of the Dudley Safeguarding Children Board and Dudley Safeguarding Vulnerable Adults Board document 'Social networking services & social media**:** Guidelines for safeguarding children, young people and vulnerable adults 2011

Other acknowledgements include;

- NSPCC Child Protection in Sport Unit Briefings

  Social Networking services, social media and sport: Guidelines for safeguarding children and young people

- Home Office Task Force on Child Protection on the Internet

  Good practice guidance for the providers of social networking and other user interactive services 2008

<u>E-Safety References</u>

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

Childline: www.childline.org.uk

Childnet: www.childnet.com

Click Clever Click Safe Campaign: http://clickcleverclicksafe.direct.gov.uk

Cybermentors: www.cybermentors.org.uk

Digizen: www.digizen.org.uk

EiS - ICT Support for Schools and ICT Security Advice: www.eiskent.co.uk

Internet Watch Foundation (IWF): www.iwf.org.uk

Kidsmart: www.kidsmart.org.uk

Teach Today: http://en.teachtoday.eu

Think U Know website: www.thinkuknow.co.uk

Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com

Section 5 - Exemplar Acceptable Use Policies

1. Staff

Purpose – addressed to teaching staff

The purpose of this document is to make sure that all staff are safe when they use the Internet through the school system and that they conduct themselves in a professional manner at all times. This includes through any equipment owned by the school or by the staff.

Personal communication

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes (or for uses deemed 'reasonable' by the Head or Governing Body).
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not use or give out my own personal details, such as mobile phone number and personal email address, to pupils or parents or for any official school communication.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that my online activity will not bring my professional role, the school or any member of the school community into disrepute.

Security

- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that personal data (such as data held on SIMS) are kept secure and are used appropriately, in school or accessed remotely and I will comply with school data protection protocols when using data on or off the school site.

- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I will ensure my password is kept secure, changed regularly and alert **XXX** (Senior Information Risk Officer) if I suspect my access has been used by someone else.

Access

- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I will not browse, download, upload or distribute any images, video, sounds or text that could upset or offend any member of the school community
- I will follow the appropriate guidelines and report any accidental or deliberate access to inappropriate materials.
- I will respect copyright and intellectual property rights.

Official school systems

- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head teacher.

This section is where schools could add any other specific policy statements

2. Secondary Schools

Purpose – addressed to teaching staff

The purpose of this document is to make sure that all students are safe when they use the Internet through the school system. This includes through any equipment owned by the school or by the student.

Personal communication

- I will only use my class email address or my own school email address when emailing
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will keep all personal information secure (e.g. home address, telephone number)
- I will only use polite language when using the computers.
- I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will not create, send or post any material that is likely to: upset or offend other people; give the school a bad name or is illegal in any way.
- I will not use language that could stir up hatred against any ethnic, religious or other minority group.
- I must actively participate in e-safety education, taking personal responsibility for my awareness of the opportunities and risks posed by new technologies.
- I will use personal devices in line with school policy.

Security

- I must keep my username and password secure.
- If I think someone has learned my password then I will tell <my teacher/technician> and change my log in details.

- I will not try to visit websites that might be inappropriate or illegal. Downloading some material is illegal and I know the police or other authorities may be called to investigate if this were done.
- I will not attempt to bypass any security settings in place on the network.
- I will not download or install any unapproved software from the Internet.

Access

- I will not use the network in any way that would disrupt use of the network by others.
- I must use only my username and password and log off after each session.
- I must make sure computers can be used by others once I log off.
- I will not attempt to harm any equipment, work of another user, or another website connected to the school system.
- I will report any websites that make me feel uncomfortable to <my teacher / a member of staff>.
- I understand that I am will not be allowed access to unauthorised chat rooms and should not attempt to gain access to them.

Official school systems

This is where you would put any school specific information. This could relate to specific equipment or systems for reporting inappropriate material.

For example:

I know that <my teacher> will regularly check what I have done on the school computers.

3. Primary Schools

Purpose – addressed to teaching staff

This document works only if a responsible adult goes through it with their class. It assumes that you use the internet even if you are an emerging reader because a lot of what you access is icon driven. The pupil agrees to this document because it will keep you safe when you are using the Internet.

Personal communication

- I will only use my class email address or my own school email address when emailing
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not give out my own details such as my name, phone number or home address.
- I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will only use polite language when using the computers.

Security

- I must not tell my username and passwords to anyone else but my parents.
- If I think someone has learned my password then I will tell <my teacher>.

Access

- I must use only my username and password.
- I must log off after I have finished with my computer.
- I will report any websites that make me feel uncomfortable to <my teacher / a member of staff>.

Official school systems

This is where you would put any school specific information. This could relate to specific equipment or systems for reporting inappropriate material.

For example:

I know that <my teacher> will regularly check what I have done on the school computers.