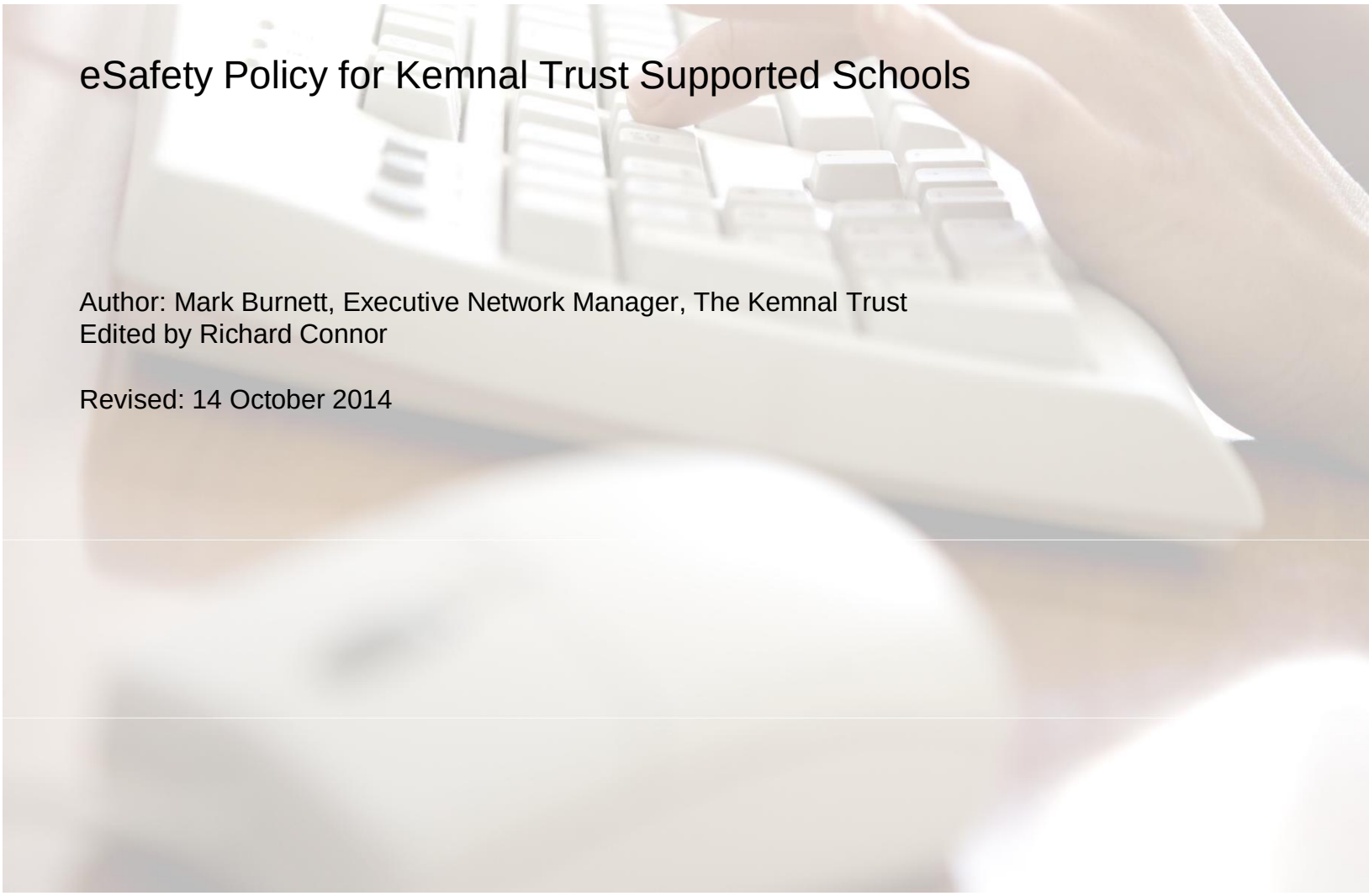


eSafety Policy for Kemnal Trust Supported Schools

Author: Mark Burnett, Executive Network Manager, The Kemnal Trust
Edited by Richard Connor

Revised: 14 October 2014

Foreword

The eSafety agenda is not an area for you to manage, not an area for me to manage, but an area that together we need to manage.

This partnership between us will help to embed the eSafety strategy in the wider work of the Kemnal Trust and its supported schools.

Mark Burnett
Executive Network Manager, The Kemnal Trust

Contents

1.0 eSafety Policy Statement

1.1 Introduction

We all have a responsibility to safeguard and promote the welfare of children, and that responsibility must apply to the online world which is such an important part of the everyday life of children and young people.

New technologies open up many exciting benefits and opportunities for children and young people but they can also present some risks. Technology is becoming all pervasive, touching all areas of society, with children and young people having increasing access to personal technology such as web-enabled phones.

We must ensure, therefore, that a framework is in place to help children and young people stay safe when using new technology, and to ensure that where problems do occur, children and young people (and their parents and carers) have support in dealing with them effectively.

1.2 Definition of Key Terms and Concepts

In this document, as in the Children Act 1989 and the Children Act 2004, a child is defined as anyone who has not yet reached their eighteenth birthday. Where we use the word 'child' (or its derivatives) in this document, we mean 'child or young person'.

Terms such as 'eSafety', 'online', 'communication technologies' and 'digital technologies', when used in this document, refer to all fixed and mobile technologies that children may encounter, now and in the future, which allow them access to content and communications that could raise eSafety issues or pose risks to their wellbeing and safety.

The term 'safeguarding' is defined for the purposes of this document in relation to eSafety as the process of limiting risks to children when using technology through a combined approach to policies and procedures, infrastructure and education, underpinned by standards and monitoring.

1.3 Disclaimer

We have made every effort to take into account relevant laws and best practice in the preparation of this policy. However, eSafety issues have the potential to be complex and versatile and, as case law in this area is still very much under development, nothing in this policy constitutes legal advice.

If you have a specific query, you should seek advice from appropriate advisors, who may include your local authority children’s services, child protection officer, the police, the Child Exploitation and Online Protection (CEOP) Centre, Internet Watch Foundation (IWF), counsellors, legal advisers, the DCSF and others.

The Kemnal Trust and its supported schools can therefore accept no liability for any damage or loss suffered or incurred (whether directly, consequentially, indirectly or otherwise) by anyone relying on the information in this policy or any information referred to in it.

2.0 Purpose of the eSafety Policy & Strategy

2.0.1 Schools have a statutory duty to safeguard and promote the welfare of children and, as technology increasingly permeates into every aspect of a child's life from an ever-younger age, eSafety must necessarily be part of this remit.

Children are now citizens born into a digital world, growing up surrounded by and immersed in the technology and tools of the digital age. Childrens access to technology has increased phenomenally in recent years: ICT is embedded in reception classrooms and is a constant and prevalent feature of school life; home access is on the increase, while connectivity from public locations such as libraries and youth clubs is now commonplace. Equally, the meeting of technologies and decreasing costs of ownership mean that, with access to a whole range of online services from mobile phones to games consoles and similar devices, children are no longer restricted to accessing the internet from a fixed location.

While it is clear that technology offers children unprecedented opportunities to learn, communicate, create, discover and be entertained in a virtual environment, there are some inherent risks. And while most children's confidence and competence in using the technologies is high, their knowledge and understanding of the risks may be low.

eSafety risks have traditionally been classified as those involving content, contact and commerce. When online, for example, children may be exposed to inappropriate content which may upset or embarrass them, or which could potentially lead to their involvement in crime and anti-social behaviour. Some people use the internet to groom children with the ultimate aim of exploiting them sexually, while ICT offers new weapons for bullies who may torment their victims, for instance using websites or text messages.

The recent surge in popularity of self-publishing and social networking sites brings new eSafety challenges, with many young people making available online some detailed and sometimes inappropriate personal information, which again raises both content and contact issues.

2.0.2 All staff providing services to children have a duty to understand eSafety issues, recognising their role in helping children to remain safe online while also supporting adults who care for children.

2.0.3 The emphasis should be very much on how to use digital technologies safely and responsibly, rather than on a blocking and banning approach.

2.0.4 It must be recognised that eSafety is not a technological issue and is not limited to settings where children have access to technology. Likewise, responsibility for eSafety is not an issue for technical staff or those with a responsibility for ICT, but must be firmly embedded within safeguarding policies, practices and responsibilities.

2.0.5 All staff who have contact with children should promote the safe and responsible use of technology in its many forms. They should learn to recognise the behaviours in children that may indicate that they are at risk from eSafety issues, and know where to go for further help. Equally, all staff should be aware of the appropriate response if a child directly divulges an eSafety incident, how to assess the safeguarding implications and how to escalate it appropriately.

3.0 Our eSafe Objectives

The Kemnal Trust and its supported schools has established an eSafety strategy with the following key objectives:

3.0.1 Ensuring that all children, young people and parents/carers are equipped with the knowledge and skills to safeguard themselves online

3.0.2 Ensuring that all children who have been the subject of indecent images and sexual exploitation are identified, protected and given an appropriate level of support

3.0.3 Ensuring that all people who work with children and young people have access to good quality procedures and effective training to safeguard children at risk through online activity

3.0.4 Ensuring that systems and services are in place to identify, intervene and divert people from sexually exploiting or abusing children online and offline.

4.0 Infrastructure Technologies Supporting Our eSafe Objectives

4.1 Overview

The schools Local Education Authority procure broadband services through local Regional Broadband Consortiums. In London, the LGfL is the RBC. The LGfL is part of the National Education Network. All English maintained schools are expected to be part of the NEN (National Education Network).

As part of our Broadband service we inherit optional functionality such as filtering and often an email provision which is constantly monitored by the provider. In all Trust supported schools we opt into the RBC's filtering service.

Whilst these services are provided for us, the majority of our infrastructure technologies reside in the schools themselves.

4.2 Our Infrastructure Technologies

In all Kemnal Trust supported schools we:

4.2.1 Maintain the filtered broadband connectivity and so connecting us to the "private" National Education Network.

4.2.2 Work in partnership with the schools LEA to ensure any concerns about the system are communicated to the broadband provider so that systems remain robust and protect students.

4.2.3 Implement additional on-site filtering providing two layers of internet security for students.

4.2.4 Complete weekly reports enabling us to monitor our anti-virus and backup solutions as well as our general network stability.

4.2.5 Apply relevant security settings to students preventing them from running unapproved applications or scripts.

4.2.6 Apply relevant security settings to staff enabling them the rights to install software, manage hardware etc.

4.2.7 Ensure that all network staff are up to date with the latest suggested practices issued by bodies such as Becta and Ofsted.

4.2.8 Ensure that all filtering methods are effective in practice and remove access to any website considered inappropriate.

4.2.9 Randomly run reports on student's internet history looking for potentially damaging and inappropriate websites.

4.2.10 Use security time-outs on Internet access where practical/useful.

4.2.11 Use individual user accounts for all students and staff.

4.2.12 Use teacher "remote management" software in all ICT suites enabling them to control/view the computers in their room.

4.2.13 Never send personal data over the Internet unless encrypted or otherwise secured.

4.2.14 Our onsite filtering service is able to block ninety percent of inappropriate content in each of the following categories:

- Pornographic, adult, tasteless or offensive material
- Violence (including weapons and bombs)
- Racist, extremist and hate material
- Illegal drug taking and promotion
- Criminal skills, proxy avoidance and software piracy.

4.2.15 There are, however, issues associated with filtering, particularly for those settings offering access to technology to a wide range of users. For example, the filtering which is necessary for a child in a public setting such as a library is unlikely to be appropriate for an adult who may be engaged in legitimate research in the same setting. Equally, there is a balance to consider between the educational value of allowing access to some sites and services in certain settings (for example, social networking sites) against the potential risks. It is doubtful, therefore, that a single filtering policy could be applied to a whole school.

4.2.16 The Kemnal Trust has addressed this by implementing three filtering policies; one for students, staff and a completely unfiltered policy for admin/testing users.

4.2.17 Students are filtered using both the on-site filtering and the provider's filtering service.

4.2.18 Staff are filtered using just the provider's filtering.

4.2.19 Unfiltered access is not assigned to any user by default but is available should the Executive Network Manager authorise it.

4.2.20 The Kemnal Trust and its supported schools do not consider filtering as a "fit and forget" solution but more an eSafety measure which needs constant evaluation.

* Other Trust policies such as "General Conditions of Use" and "Information Security" detail our network management strategy and how we deliver ICT to the end user. This can be downloaded from our website or found on the desktop of all staff users. *

4.3 Monitoring and Reporting

The Kemnal Trust monitors its network infrastructure regularly and consistently. We particularly track and identifying trends in advance of eSafety and security issues arising.

If eSafety incidents do occur, our robust technological infrastructure can provide evidence and activity trails.

Additionally, our General Conditions of Use Policy state what monitoring and reporting of individual usage is in place. Not only can this help to encourage a culture of safe and responsible behaviour, but also transparency of approach is important to alert users to their rights to privacy (which may help to avoid complications should eSafety incidents occur).

4.4 Network Staff

Network staff in Kemnal Trust supported schools each receive support in their roles. They attend regular training in eSafety issues and are clear about the procedures they must follow if they discover, or suspect, eSafety incidents through monitoring of network activity.

5.0 Responding to an eSafety Incident

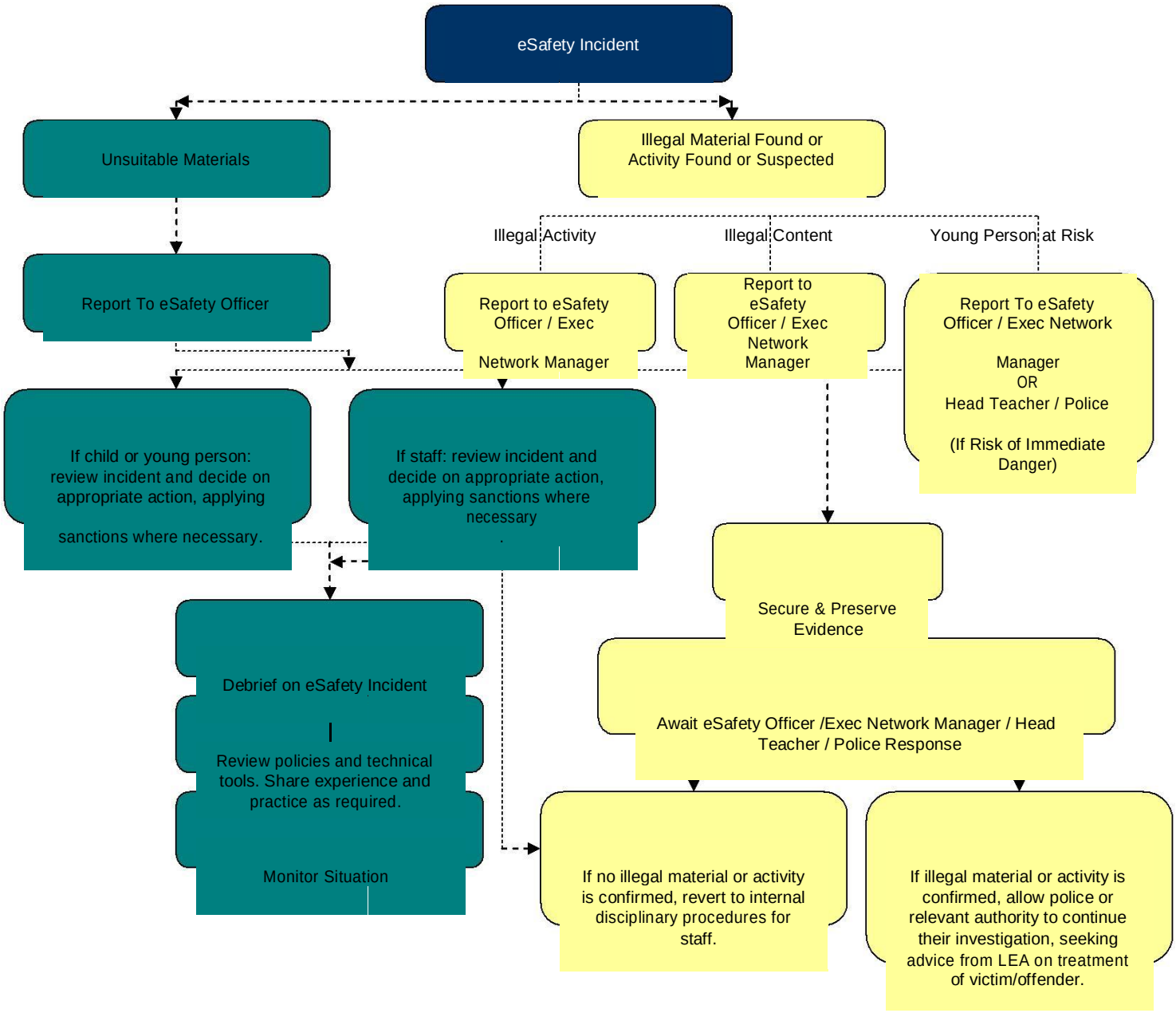
Technological solutions to eSafety can never be 100 per cent effective and, unfortunately, there may still be occasions when eSafety incidents do occur. There should therefore be clear lines of communication for reporting specific incidents, and this should include escalating incidents, involving other agencies and disclosure.

5.0.1 When developing this policy, considerations were made to various eSafety scenarios, responses and reporting mechanisms. Examples include:

- Accidental access to inappropriate material
- Deliberate access to inappropriate material
- Accidental access to illegal material
- Deliberate access to illegal material
- Inappropriate or illegal use of email
- Inappropriate or illegal use of other technologies
- Deliberate misuse of the network (for example, hacking or virus propagation)
- Bullying or harassment using technologies
- Sexual exploitation using technologies.

5.0.2 Depending on the nature of the event, different eSafety incidents will require different responses, and undoubtedly no two eSafety incidents will be exactly the same. This does not mean, however, that responses should be left to chance and circumstance: instead The Kemnal Trust and their supported schools modeled general processes and procedures for responding to incidents, drawing on good practice within the wider field of child protection as appropriate.

5.0.3 Responding to an eSafety Incident Flow Diagram



5.0.4 A key requirement in responding to eSafety incidents is to recognise when to escalate incidents. This involves recognising when to involve other agencies (such as social care, the police, the Internet Watch Foundation (IWF), or the Child Exploitation and Online Protection (CEOP) Centre) and securing and preserving evidence correctly.

In particular, staff must be aware of the local procedures to follow should eSafety incidents arise. This will include how and when to contact external agencies.

6.0 Responsibilities

6.0.1 The schools eSafety officer and the Trusts Executive Network Manager are responsible for maintaining the eSafety policy and providing adequate training/awareness.

6.0.2 The schools eSafety officer and the Trusts Executive Network Manager will carry out regular audits of the filtering service to ensure that the school provides a secure environment for its users.

6.0.3 The schools eSafety officer will ensure that pupils and staff are adhering to this policy and any incidents of possible misuse are investigated.

6.0.4 The schools eSafety officer will ensure that eSafety is included in the curriculum for all students highlighting the requirement for safe and responsible use.

6.0.5 The schools HR department will ensure that all staff signs the relevant documentation to confirm that they acknowledge and agree to adhere to the policies in place within the school/Trust.

6.0.6 In all Trust supported schools, the act of logging on indicates acceptance to the policies in place within that school. This is presented as a message to all users attempting to logon.

6.0.7 The eSafety policy and all other ICT policies are available on request to all students, staff, parents, governors and visitors. Any issues or queries with any of these policies should be raised immediately with the schools eSafety officer or the Trusts Executive Network Manager.

7.0 eSafety Contacts

AREA IT MANAGER
CONNORR@WELLINGSCHOOL-TKAT.ORG

8.0 Legal Framework

This section is designed to inform users of legal issues relevant to the use of electronic communications. It is not professional advice.

Many young people and indeed some staff use the Internet regularly without being aware that some of the activities they take part in are potentially illegal. The law is developing rapidly and recent changes have been enacted through:

- The Sexual Offences Act 2003, which introduces new offences of grooming, and, in relation to making/distributing indecent images of children, raised the age of the a child to 18 years old;
- The Racial and Religious Hatred Act 2006 which creates new offences involving stirring up hatred against persons on religious grounds; and
- The Police and Justice Act 2006 which extended the reach of the Computer Misuse Act 1990 making denial of service attacks a criminal offence.

8.1 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.

8.2 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).

8.3 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. Children, Families and Education Directorate page 37 April 2007

8.4 Data Protection Act 1998

The Act requires anyone who handles personal information to notify the Information Commissioners Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

8.5 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.

8.6 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.

8.7 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 authors own creation and the result of some skill and judgment. 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 anyones work without obtaining the authors permission. Usually a license 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 license before you copy or use someone else's material.

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

8.8 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. Children, Families and Education Directorate page 38 April 2007

8.9 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 a 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.

8.10 Obscene Publications Act 1959 and 1964

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

8.11 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.

8.12 Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIP) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998.

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.

The Kemnal Trust

eSafety – Hints and Tips for adults working with children and young people.

Read this, it might be helpful …

Social Networking hints and tips

Social networking sites are brilliant ways to stay in touch with friends and share photographs, comments or even play online applications such as chess or word games. However, they are also designed to enable advertisers to target you and entice you into buying goods and services based on the 'profile' information you reveal. Be web savvy!

- Social networking sites, such as Facebook, have a range of privacy settings. These are often set-up to 'expose' your details to anyone. When 'open' anyone could find you through a search of the networking site or even through a Google search. So, it is important to change your settings to "Just Friends" so that your details, photographs etc., can only be seen by your invited friends.
- Have a neutral picture of yourself as your profile image. Don't post embarrassing material.
- You do not need to accept friendship requests. Reject or ignore unless you know the person or want to accept them. Be prepared that you may be bombarded with friendship requests or 'suggestions' from people you do not know.
- Choose your social networking friends carefully and ask about their privacy controls.
- Do not accept 'friendship requests' on social networking or messaging sites from students, pupils or young people (or their parents) that you work with. Remember ex-pupils may still have friends at your school.
- Exercise caution – for example in Facebook if you write on a friends 'wall' all their friends can see your comment – even if they are not your friend.
- There is a separate privacy setting for Facebook groups & networks, you might have your profile set to private, but not for groups & networks. If you join a group or network everyone in the group or network will be able to see your profile.
- If you have younger family members on your social networking group who are friends with your students or pupils be aware that posts that you write will be visible to them.
- If you wish to set up a social networking site for a school project create a new user profile for this, do not use your own profile.
- If you or a friend are 'tagged' in an online photo album (Facebook, Flickr or similar) the whole photo album will be visible to their friends, your friends and anyone else tagged in the same album.
- You do not have to be friends with someone to be tagged in their photo album.
- If you are tagged in a photo you can remove the tag, but not the photo.
- Photo sharing web sites may not have privacy set as default.
- Your friends may take and post photos you are not happy about. You need to speak to them first, rather than contacting a web site. If you are over 18 the web site will only look into issues that contravene their terms and conditions.
- Once something is on the internet, even if you remove it, the chances are it has already been snapshotted by a 'web crawler' and it will always be there. Archives of web content are stored on sites like the WayBackMachine.
- Think about your internet use, adults are just as likely to get hooked on social networking, searching or games. Be aware of addictive behaviour!
- You will not be able to remove yourself completely from the Internet. 192.com has all the English electoral roles and for as little as £9.99 your personal information can easily be found by a stranger.

Wider Internet hints and tips

- Never tell anyone your password.
- Be careful how you choose passwords, most are very predictable. It is easy to find personal details online that might give password clues. It is recommended that you include capital letters, lower case letters and numbers – avoid birthdates, names, pets, addresses etc. It is best to avoid any words found in a dictionary.
- Keep all professional work and transactions completely separate from private. Create a web-based email account for private online business, such as online shopping and ensure you use your school / work email only for any professional communications.
- Create yourself a hotmail (or similar) account to use when searching for insurance quotes etc, when you are done either close the email account, or ignore it. Any junk mail generated will then not affect you.
- Be careful when form filling online…., do you know who the data is for? Only answer 'required 'questions, do not just give out information because you have been asked for it.
- Never verify banking details online.
- When you need to use a 'name' online consider what name you use. In a professional context you would probably use your full name, but in other contexts you may decide to use an alias to protect your identity. If so make sure it is appropriate.
- If you create a family tree and post it on the Internet, make sure your tree is set to private for anyone living or recently deceased (last 50 years). The information posted would be enough for someone to steal your identity and probably guess passwords and common security questions.
- If you get a phone call or an email from someone asking you to confirm personal details, (unless you are expecting the contact) do not give out any personal information.
- Popup adverts are often a nuisance. Close them carefully as a 'close' button will often lead you to more advertising as the 'X' may be a link to further nuisance sites.
- If you get an email or popup offer that seems too good to be true it probably is! Watch out for online cons – it is like online door step selling.
- If someone sets things up for you at home, make sure you change your password immediately. Someone with your username and password could impersonate you.
- If you think someone is impersonating you on Facebook or similar, report it. Impersonation usually breaches the terms and conditions – you will need to know the specific URL or user name, sites cannot work from a hunch.
- Cookies are not necessarily a bad thing. They save your surfing information and speed-up access to sites. However, if someone else has been surfing 'adult content' on your computer, the stored cookies may mean you get 'adult pop-ups and adverts'.
- Use legal sites for downloading music, films etc., such as iTunes.
- File sharing sites are not illegal but sharing of copyright material is. Downloading of illegal music and film downloading also leaves you at a huge risk of viruses. Even if you subscribe to a file sharing web site, such as Limewire, it does not mean that your downloading becomes legal.

- You can get Internet access from many games consoles and some MP3 players. Games with multiplayer features are often labelled as 'net play'. This means that you are playing with strangers online – the risks here are the same as for social networking, chatrooms and messengers.
- Applications like Skype and iplayer need bandwidth and can slow down the internet, particularly if you use a 3G mobile stick. Full screen iplayer could use up your allocation and your service may be 'throttled' - meaning you can only do some basic text work, searching and emails, but picture and video will not be possible.
- When you log-into a web site, unless your computer is exclusive to you, don't tick boxes that say 'remember me'.
- Don't leave yourself logged into your computer, software or websites. If you have to move away from your computer, log out.
- Don't give your username and password to anyone such as to a supply teacher / temporary member of staff – make sure your school has a guest login for visiting staff.
- Your school or work laptop (or other equipment) should not be used by friends and family.

If you work with young people:

- Try to provide pupils with direct links embedded into 'pages' in a document, London MLE 'room', or interactive whiteboard resource etc.
- If you do need to undertake Internet searches (including Internet image searches), rehearse before you use in class. Think about search terms. Even the most innocuous term can bring up adult material.
- Use child-friendly search engines with younger pupils. Older young people will use a variety of search engines at home, you are a role model for them in good use of a search engine. Look for opportunities to teach young people how to use search engines.
- When checking out web content make sure you are not displaying it on the interactive whiteboard or via a projector – research away from pupils.
- Watch YouTube (or any) videos before you use them in the classroom.
- If you use a YouTube (or any) videos, find out how to embed it using the 'Source' rather than a page link, as that exposes pupils to other content.
- If you cut and paste or save content from the Internet or other peoples files make sure you remove the hyperlinks embedded in the text, or attached to images.
- If you want to use a clip download it (if legal & copyright allows), it might not be there next time you look for it.
- If you use your own equipment in school (such as cameras or laptops), ensure senior leadership have given you permission and make sure that school files (photographs etc) are downloaded and stored in school, not at home.
- Do not take stored pupil photos or information home. If for any reason you need to ensure you have senior leadership's permission, and ensure it is on an encrypted device.
- Video Conferencing – you can be broadcasting without realising it, if you have VC in your classroom make sure it is switched off after use and that the camera is turned away from the class.
- You need to be a role model for copyright. Make sure you use multimedia resources appropriately, don't just 'grab stuff' off the Internet. Use the copyright images from the NEN, LGfL or other sites your school / LA has advised you of. You cannot show DVDs in school, although it is safe to use film trailers. But, make sure you download the right version, as there are can be more than one film trailer, including trailers for 'adult versions' of blockbusters.

Email hints and tips

- Keep all professional work and transactions completely separate from private. Create a web-based email account for private online business, such as online shopping and ensure you use your school / work email only for any professional communications.
- Create yourself a hotmail (or similar) account to use when searching for insurance quotes etc, when you are done either close the email account, or ignore it. Any junk mail generated will then not affect you.
- If you get an email from someone or a company that you have never head of and it asks you to reply to unsubscribe, don't. By unsubscribing you will verify that you exist. Just ignore the email. If they carry on emailing use email rules to block the sender.
- If you get emails that offer you money making schemes (e.g. the 'Nigerian email'), Russian wives, pharmaceutical products and body part enhancement don't be upset, you have not been personally targeted, this is spam and junk mail.
- Webmail is useful but insecure, and your email address is easily passed on.
- If you get spam or junk mail it does not mean that someone has 'hacked' into your email; people get email addresses in different ways, it might be a software 'guess' – a programme generates lots of possible emails and sends out millions of emails knowing that statistically some of them will be real. Software also searches web sites for email addresses and harvests them.
- Only open Email attachments from trusted sources, you won't get a virus from the initial email text, but it may be contained in an attachment.
- If emails from friends or acquaintances start to become unsuitable – say something before you receive something really problematic.
- Don't give out private email addresses to students and pupils.

Phone hints and tips

- Don't give out your mobile number or home number to students or pupils.
- If you have a Bluetooth phone do you know if Bluetooth is turned on or off? If it is on is there a password? Open un-passworded Bluetooth means anyone else with Bluetooth in range can read the content of your phone or device.
- Many hand held games consoles have wireless and Bluetooth and can be used to make contact from 'stranger' devices within range.

For more information, please contact:

Richard
Connor

IT AREA NETWORK MANAGER, The Kemnal Trust

e: connorr@wellingschool-tkat.org

w: www.wellingschool-tkat.org