Safer Professional Practice with Technology

September 2016

kent.gov.uk

Disclaimer

Kent County Council (KCC) makes every effort to ensure that the information in this document is accurate and up to date. If errors are brought to our attention, we will correct them as soon as practicable. Nevertheless, KCC and its employees cannot accept responsibility for any loss, damage or inconvenience caused as a result of reliance on any content in this publication

This document is available in a range of formats and can be explained in other languages. To ask for an alternative version, please email alternativeformats@kent.gov.uk

Kent County Council Equality and Diversity Team, phone with Type Talk: 18001 03000 421553

Or write to: *Kent County Council, Diversity & Equality Team Room G37, Sessions House, County Hall, Maidstone, Kent, ME14 1XQ*

Contents

Introduction: Safer Professional Practice with Technology

“e-Safety” or online safety covers issues relating to children, young people and adults, and their safe use of the Internet, mobile phones, tablets and other electronic communications technologies, in a range of settings including schools, early year’s providers, local sport clubs, youth groups and libraries as well as within the home. The online safety agenda has shifted towards enabling users to manage risk and develop resilience, rather than relying on filtering to block content and “remove” hazards. This change of perspective requires professionals to develop a greater understanding of the “online world of the child” as well as within their own personal and professional life and acknowledge that we must all be empowered and educated to be better equipped with the skills to make safe and responsible decisions online.

The Kent e-Safety Strategy group, on behalf of the Kent Safeguarding Children Board (KSCB),. comprising multi-agency professionals from across the Kent children’s workforce to help professionals make informed and appropriate choices about technology, has developed this guidance which seeks to help professionals working with children and young people (those aged up to 18) and their families to ensure that their use of technology is safe and appropriate.

This document will be appropriate for a range of professional organisations including but not limited to schools, early years settings, colleges, social care, early help settings, children’s homes, voluntary organisations, police, charities, libraries etc. It may also be appropriate for other organisations working with vulnerable groups. All agencies will have different requirements, expectations and client groups as well as statutory requirements or responsibilities and agency leads must ensure that the content is suitably adapted or amended to meets any specific organisational needs or expectations.

All adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust. This document discusses appropriate and safer behaviours for adults working in paid or unpaid capacities in a professional context.

A simplistic rules approach will not resolve complex issues but local and national legislation and guidance, including the Kent Safeguarding Children Board Procedures should be followed at all times. This document suggests a set of real situations to enable professionals to develop greater awareness of the dangers and to consider consequences of behaviour earlier in a developing situation.

This document has been based in part upon the October 2015 “Guidance for safer working practice for those working with children and young people in education settings” document from the safer recruitment consortium. This document can be accessed here:
www.kelsi.org.uk/__data/assets/pdf_file/0016/46510/Guidance-for-safer-working-practice-working-in-education-October-2015.pdf

Aims of the document

This document aims to:

- Ensure safeguarding children and young people online is a priority.
- Assist adults to work safely and responsibly and to monitor their own standards and practice.
- Help adults to set clear expectations of their own online behaviour and to comply with staff codes of conduct.
- Minimise the risk of allegations being made against adults about inappropriate behaviour.
- Project a clear message that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or criminal action will be taken.
- Support managers and leaders in establishing a culture which safeguards both staff and young people online within their organisation.

Managers and designated safeguarding leads (DSLs) must ensure they are clear about their own expectations regarding what the organisation considers to be safe and appropriate use of technology and must ensure that this is clearly communicated with all members of staff, including volunteers. This is essential in order to safeguard all members of the community.

Kent education settings can contact the Education Safeguarding Adviser (Online Protection) to discuss safe practice: esafetyofficer@kent.gov.uk and further information regarding online safety can be found at www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding/e-safety

Suggestions for use

It is recommended that leaders and managers consider using this document via a range of options, as appropriate to their staff, to ensure that professionals are aware of the issues and the implications.

Possible options to consider are:

- Clear references within existing organisational policies/procedures/guidance on the safe and appropriate use of technology
- Provide copies of or links to this document to all members of staff as part of induction
- Place copies of or links to this document in staff areas e.g. the staff room, intranet systems
- Provide copies of or links to this document to all members of staff alongside the code of conduct/Acceptable Use Policy (AUP) and request that staff sign to confirm that they have read and understood appropriate documents
- Use some of the statements within a staff development or training session and discuss some of the issues and implications highlighted

Questions for further discussion

The following questions might be used by Designated Safeguarding Leads (DSLs) to initiate further staff discussion:

- Can I use a work computer to book holidays during my lunch time or after work?
- Can I respond to a comment about my workplace via my personal social networking account?
- Should I use my personal email address or phone number to contact children, young people, parents or other professionals?
- Can I use my smartphone to “tweet” on behalf of my organisation?
- Is it okay to use social media to teach children and young people how to keep safe online?
- Can I use my personal smartphone to access my work emails?
- Can I comment on local or political news stories on social media?
- Can I create a “blog” (Online journal) or a “vlog” (video journal) and mention my work?
- What privacy settings are available on your social networking sites?
- I’ve seen a colleague post comments online that I think are inappropriate, what should I do?
- How can I use social media safely as a professional (e.g. for my own CPD)?

If in doubt, all professionals are encouraged to:

- Consult with their line manager and organisation policies.
- Consult with their agency lead for safeguarding.
- Consider how an action would look to a third party.
- Only publish content online that they would be happy to share with parents, children and young people and their employer.

Please be aware that this guidance is subject to change following local and national legislation.

Frequently Asked Questions: Keeping Children and Young People Safe Online

Please be aware that staff must always follow their organisations appropriate policies e.g. codes of conduct, acceptable use policies (AUPs), safeguarding report mechanisms etc.

What risks should I be aware of for children and young people online?

In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children and young people (and indeed adults) in danger. Childrens workforce professionals must acknowledge the role and influence of technology when working with children and be able to recognise, respond to, record and refer any online safety concerns.

Children and young people are likely to encounter a range of risks online which can be highlighted as

- **Content:** being exposed to illegal, inappropriate or harmful material
- **Contact:** being subjected to harmful online interaction with other users (peers and strangers)
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm

These issues can be summarised as:

	Commercial	**Aggressive**	**Sexual**	**Values**
Content Child as recipient	Advertising Spam Copyright Sponsorship Hacking	Violent content Hateful Content	Pornographic content Unwelcome sexual comments	Bias Racist and extremist content Misleading info/advice Body Image and self esteem Distressing or offensive content Neglect
Contact Child as participant	Tracking Harvesting data Sharing personal information	Being bullied, harassed or stalked	Meeting strangers Sexualised bullying (including 'sexting') Grooming Online Child Sexual Exploitation	Self-harm and suicide Unwelcome persuasions Grooming for extremism and radicalisation
Conduct Child as actor	Illegal downloading Hacking Gambling Privacy Copyright	Bullying, harassing or stalking others	Creating and uploading inappropriate or illegal content (including 'sexting') Unhealthy/inappropriate sexual relationships Child on child sexualised or harmful behaviour	Providing misleading information and advice Encouraging others to take risks online Sharing extremist views and radicalisation Problematic Internet Use or "Addiction" Plagiarism

Content adapted from EU Kids Online 2008

It is important to recognise that online abuse can be perpetrated by children and young people and family members as well as by strangers.

What is classed as ‘inappropriate’?

Inappropriate is a term that can mean different things to different people. It is important to differentiate between ‘inappropriate and illegal’ and ‘inappropriate but legal’. All staff should be aware that in the former case accessing illegal content investigation may lead to criminal investigation, prosecution, dismissal and barring. In the latter it can still lead to disciplinary action, dismissal and barring even if there is no criminal prosecution.

Illegal

- Accessing (viewing), making, storing (possessing) or disseminating indecent images of children on or off the internet, whether on or off work premises is illegal (Protection of Children Act 1978, section 1,1,a and Criminal Justice Act 1988, section 160) If proven, this will lead to criminal proceedings and the individual being barred from working with children and young people.
- Possessing or distributing incident images of a person under 18 can include viewing such images online; this may also constitute possession even if they are not saved. What is regarded as indecent would ultimately be down to a jury to decide. The police have a grading system for different types of indecent image. Remember that children and young people may be harmed or coerced into posing for such images and are therefore victims of child sexual abuse and exploitation.
- This also applies to indecent images created by children and young people (those aged under 18) themselves and is often referred to as “sexting”. KSCB guidance for professionals regarding responding to youth produced sexual imagery or sexting can be found here: www.kscb.org.uk/guidance/online-safety
- Staff must **NEVER** print, save, forward etc. anything they suspect to be an indecent image of a child. Devices and systems thought to contain indecent images should be immediately secured or contained (in line with the organisation safeguarding/online safety policy) and police advice should be sought.
- Sharing adult pornography with children (under 18) is also illegal (Sexual Offences Act 2003, section 12).
- The offence of grooming is committed if someone over 18 has communicated with a child under 16, at least twice (including by phone or using the Internet) and meets them or travels to meet with them anywhere in the world with the intention of committing a sexual offence. (Sexual Offences Act 2003, section 15)

Illegal Hate/Harm/Harassment

- General: There is a range of offences to do with inciting hatred on the basis of race, religion, sexual orientation etc.
- Individual: There are particular offences to do with harassing or threatening individuals – this includes cyber bullying by mobile phone, social networking sites etc. It is an offence to make credible threats or send offensive messages with the purpose of causing the recipient distress or anxiety.

Please be aware that this list is not exhaustive and advice should always be sought if professionals suspect a criminal offence has taken place

Examples taken from real events:

- Staff sending sexualised messages to children and young people
- Staff showing children pornographic content
- Staff printing, saving or forwarding indecent images of children or young people
- Children, young people and professionals being sent racist or homophobic comments or threats to hurt
- Staff forming sexual relationships with children or young people

Inappropriate

Think about inappropriate in respect of your professionalism and being a role model. The scope for inappropriate content and behaviour is enormous, but bear in mind that actions outside of the workplace could be so serious as to fundamentally breach the trust and confidence placed in the employee and may constitute gross misconduct.

Examples taken from real events:

- Posting offensive, derogatory or insulting comments about the colleagues, children, young people, families or the organisation/agency on social media
- Using a work email address to register for online dating services
- Accessing adult pornography on work devices and computers during break
- Liking or sharing extremist views or content on social networking sites
- Using personal devices for personal use (e.g. checking social media or online shopping) whilst supervising children
- Staff sharing drunken photos online
- Contacting children or young people via personal email address or social media channels
- Trading in sexual aids, fetish equipment or adult pornography

How do I ensure safer online activity when working directly with children and young people?

Most internet use is likely to be safe, purposeful and beneficial to children, young people and professionals. However, there is always an element of risk; even an innocent search can occasionally turn up links to adult content or imagery. Professional working within the community (such as within family homes) should be aware that filtering may not always be in place so additional degrees of caution will be required.

Planning and preparation is vital and the safest approach when using online material with children is to always check sites and services before use with children and young people. Professionals should be aware that the internet is dynamic and content perceived as “safe” today might not be as “safe” tomorrow.

For younger children, staff should direct them to a specific website or a selection of pre-approved websites and avoid using search engines. When working with older children, staff should select an appropriate and

safe search engine and ensure safe search settings are in place. Staff should however be aware that this only reduces and doesn't remove the risk of children and young people accessing unsuitable content, especially when searching for images or videos. Appropriate search terms should be used and pre-checked. Staff should consider carefully the age, ability and maturity of all children when planning online activities.

When encouraging children or young people within education settings to publish work online, professionals should ensure that age appropriate sites and services are used at all times. If using online video clips, professionals must ensure that the video is clear of any unsuitable content (including links and adverts), and know how to flag and report any concerns.

If inappropriate material is discovered then, turn off the monitor/screen, reassure the child/young person and to protect yourself, log and report the URL in line with your organisations policy e.g. to a member of senior staff. Professionals should avoid printing or capturing any inappropriate material and must not print, forward or save illegal content.

I'm working with a family who wants help to keep their children safe online, what resources are available to help them?

Parents and carers are an essential part of keeping children and young people safe online. Most internet access takes place when children and young people are within the home therefore it is essential that parents/carers are aware of their children's internet use and implement appropriate measures to safeguard them online.

Technology can sometimes be seen as a "scary" or "frightening" for many parents and carers as they may be concerned about not having sufficient computer skills to help protect their child. This fear can prevent parents/carers from taking appropriate measures to safeguard their children, which unlimitedly puts them at risk of harm. The important part of online safety is however not about having technology knowledge, it is about keeping children and young people safe, therefore parenting and communication skills are more important.

Sometimes families may think they are doing enough to protect their children by using parental controls, putting filters on search engines, installing antivirus software, having a laptop downstairs and banning children from using certain sites without considering how successful these tools are or if their children could access the internet elsewhere, so it is important to highlight that discussion and education about safe use is the key

The following links will have a range of useful resources for professionals to use and share with parents/carers:

- www.thinkuknow.co.uk
- www.internetmatters.org
- www.saferinternet.org.uk
- www.childnet.com

- www.nspcc.org.uk/onlinesafety
- www.net-aware.org.uk
- www.getsafeonline.org
- www.parentzone.org.uk
- www.parentsprotect.co.uk
- www.parentinfo.org

If parents/carers request help for specific concerns then professionals should consult with their agency lead for safeguarding who may be able to signpost to specific resources.

I'm aware a child or young person is using a popular social media site but they aren't the correct age – is this illegal?

No. The age limits for popular social networking sites are set to 13 (sometimes higher) due to the Children's Online Privacy Protection Act of 1998 (COPPA) which is a United States federal law. COPPA applies to any websites, apps or online services which collect, store or use personal information under U.S. jurisdiction from children under 13 years of age. COPPA legislation details what a website operator must include in their privacy policy, when and how to seek verifiable consent from a parent or guardian, and what responsibilities an operator has to protect children's privacy and safety online including restrictions on the marketing and advertising to those under 13. Whilst children aged under 13 can legally give out personal information with their parents' permission, many websites disallow underage children from using their services altogether due to the cost and work involved in the law compliance. This is why most popular social networking sites (such as Facebook, YouTube, Twitter, Instagram etc.) have an age restriction of at least 13+. It is very easy for children and young people (or indeed adults) to enter an incorrect date of birth or false information to open a false or imposter account when registering for a social networking site as it is impossible for sites to verify every user. This is not a criminal offence.

It is however very important to recognise that if we simply report, ban or instruct children and young people not to use social networking sites then we will run the risk of driving any problems or incidents such as abuse or bullying underground. This can in some situations be more dangerous that the use of social networking in the first place. Whilst professionals must be careful not to condone or promote the underage use of social media, we must recognise that children, young people and their parents/carers may need further information and support to make informed and appropriate choices.

All adults should ensure that all children and young people understand how to behave online in all circumstances and these skills should carry over to whichever site or system they are using.

There are some useful websites which can be used to help professionals explore these issues with children, young people and families:

- The Australian Office of the Children's e-Safety Commissioner created a useful infographic which highlights some age restrictions (along site the app store rating) for some popular apps and tools which can be found here: www.kentesafety.wordpress.com/2016/06/01/is-there-an-age-limit-for-kids-on-social-media-infographic-from-the-australian-childrens-e-safety-commissioner/

- The NSPCC's Net Aware Service also rated and reviewed over 50+ popular social media apps and services: www.net-aware.org.uk

- www.thinkuknow.co.uk and www.safeinternet.org.uk have useful advice and practical information for children, young people and parent/carers to help them make informed choices about social media, how to use privacy settings and how to report concerns.

If you believe that a child or young person is at risk of significant harm as a result of the underage use of social media such as they are sharing personal information or posting offensive or provocative content then you may need to consider if the child or young person and family requires specific intervention or support. Professionals should consider sharing their concerns about the child's use of social media with the parents/carers and see if they can understand the concerns that you have relating to their child's behaviour and see if they can take appropriate action to safeguard their child.

If parents/carers fail or refuse to protect their child once a concern has been raised with them then professionals will need to consider if other agencies need to be involved, for example via early help or children's social care. This is more likely to be the case for younger children or if there has been a serious incident linked directly to use of social media. In these situations professionals must always follow their organisations safeguarding policies and procedures and should speak to their DSL immediately if they believe a referral is required.

I'm aware that a child or young person is playing 18 rated video games – should I tell the police?

No, it's not illegal for children or young people to play 18+ games; it's only illegal for the shop to sell the game directly to them. If you are made aware of children or young people playing games that are not suitable for them, then the most important thing is to focus on raising parents' awareness about the possible risks etc. and to educate the child/young person about appropriate on and offline conduct.

The actual impact of 18+ video games on children and young people is widely debated and often inconclusive or conflicted. Some studies suggest that the impact of playing 18+ video games may depend on if the child/young person is already pre-disposed to violence and suggests that there is often a range of other factors involved, including family environment, age, ability etc. and awareness and education about the potential impact is usually the best solution. It may be useful to discuss age ratings with parents and children/young people to help them make informed decisions and how to put parental controls in place.

Useful links to use with families regarding video games and online gaming include:

- www.pegi.info/en/index
- www.childnet.com/parents-and-carers/hot-topics/gaming
- www.childnet.com/resources/online-gaming-an-introduction-for-parents
- www.net-aware.org.uk
- www.saferinternet.org.uk/advice-and-resources/parents-and-carers/parents-guide-to-technology
- www.internetmatters.org

If you believe that a child or young person is at risk of significant harm as a result of gaming such as they are displaying violent, aggressive or sexualised behaviour, which can specifically be link to a game then you may need to consider if the child or young person and family requires specific intervention. Professionals should consider sharing their concerns about the child's use of gaming with the parents/carers and see if they can understand the concerns that you have relating to their child's behaviour and see if they can take appropriate action to safeguard their child.

If parents/carers fail or refuse to protect their child once a concern has been raised with them then professionals will need to consider if other agencies need to be involved, for example via early help or children's social care. This is more likely to be the case for younger children or if there has been a serious incident linked directly to exposure to an 18+ video game. In these situations professionals must always follow their organisations safeguarding policies and procedures and should speak to their DSL immediately if they believe a referral is required.

A child or young person has told me that they are being bullied online. It's happening at home, so whose responsibility is it?

The responsibility for dealing with online bullying is shared. It will require cooperation between children, young people, parents, professionals and schools/education settings to ensure that situations are identified and managed appropriately.

Online or cyberbullying is the use of technology particularly mobile phones and the internet to deliberately upset or harass someone. Whilst in theory cyberbullying is just another form of bullying, it can be different to traditional bullying. Online bullying can take place anytime, anyplace and this can create a feeling of there being 'no escape' for the victim. Online bullies can attempt to be anonymous and can feel distanced from the incident. They are often unaware of the laws regarding harassment and the fact online activity can be traced via digital footprints. Electronic content is very hard to control once it has been posted and can never be guaranteed to be removed totally from circulation - this can be very upsetting to victims as they can never be sure who has viewed images or content about them. Online bullying can sometimes occur unintentionally, often due to a lack of awareness or empathy e.g. "It was only a joke". Bystanders can easily become perpetrators of online bullying by liking or sharing videos, images or content and a one off comment can become bullying due to the repeated and permanent nature of the internet. Online bullying can sometimes even be perpetrated by the victim themselves (known as Digital Self-Harm).

Although bullying in itself is not a specific criminal offence in the UK, it is important to bear in mind that some types of harassing or threatening behaviour or communications could be a criminal offence, for example under the Protection from Harassment Act 1997, the Malicious Communications Act 1988, the Communications Act 2003, and the Public Order Act 1986. If a professional believes that a crime has been committed then they should seek assistance from the police via 101. If it is an emergency (if someone is injured, in danger or there is a risk to someone's life) then you should contact 999.

If a child or young person discloses online (or cyber) bullying to you then the first response should be to support them and reassure them that they have done the right thing by reporting the bullying. You should

advise them how to deal with bullying appropriately, for example how to block bullies or report the users to the website. They should be instructed to keep evidence by taking screen prints or keeping messages (including times, dates, names and locations if possible), not to retaliate and to tell a trusted adult.

If the child or young person is being bullied by known individuals such as peers then school and educations settings should be involved and support and sanction children according to their anti-bullying and behaviour policies. Section 89(5) of the Education and Inspections Act 2006 gives headteachers the power to regulate pupils' conduct when they are not on school premises and are not under the lawful control or charge of a member of school staff. This can relate to any bullying incidents occurring anywhere off the school premises (including online) and if bullying outside of school involving pupils is reported then it should be investigated and acted on.

What should I do if a child or young person discloses online abuse?

It is essential for professionals to recognise the importance of a child or young person disclosing an online safety concern. Typically children and young people are fearful of talking about online dangers with adults as they either believe the adult will dismiss the issue e.g. '*I don't understand technology, I wish it could be banned*' or from for fear of being punished by having their devices taken away or their access to the internet removed. It is essential for professionals to acknowledge that online safety concerns are just as serious as "real life" concerns. We must also be aware that the removal of devices or attempting to prevent internet access will not always solve online safety issues, and in some cases can make situations worse as children and young people will lie about or hide their behaviour which leads to them being more vulnerable online.

Dealing with disclosures about online abuse should be responded to in much the same way as offline disclosures, although in some cases additional queries about sites and services involved or collection of evidence will be required or recommended.

You should always follow your organisations policies and procedures if a child or young person makes a disclosure. You should ensure you do not promise confidentiality and must explain what you are going to do with the information they have shared with you and why. Professionals are often cautious of asking questions; however in some cases it may be appropriate, for example if you need to clarify information e.g. Tell me…, Explain what…, Describe how…

Professionals should not ask questions to gather opinions (e.g. why did you do that) as that can make children feel that they are to blame. Staff must never request that a child or young person prints, saves or forwards any images or content which is thought to be an indecent image of a child.

The first point of contact following a disclosure by a child or young person should be the designated safeguarding lead within your organisation - professionals should not attempt to handle online abuse situations alone. You should write down the disclosure as soon as possible and using the child or young person's own words.

The child or young person should be reassured and supported at all stages and involved as far as is possible (according to their age and ability), for example speaking to the safeguarding leads, reporting concerns.

Social workers working with children or young people who have made disclosures regarding online abuse should follow child protection Section 47 enquiry procedures. The purpose of the Section 47 enquiry is to determine whether any further action is required to safeguard and promote the welfare of the child or children who is/are the subject of the enquiry.

I'm working with a child, young person or family who have experienced a specific concern online – is support available for them?

There are a range of external agencies which may be helpful to provide specific support to children, young people and families.

CEOP: www.ceop.police.uk and www.thinkuknow.co.uk

- The NCA's CEOP Command (formerly the Child Exploitation and Online Protection Centre) delivers a multi-agency service dedicated to tackling the abuse and exploitation of children in the real and the "e" world. A key focus of CEOP is the Think U Know website and education strategy to teach young people, professionals and parents/carers about e-Safety and has a "Click CEOP" report abuse button to report online abuse or suspicious behaviour. Any reports of abuse made via CEOP's or the VGT 'Report Abuse' button will be answered 24 hours a day, 7 days a week from around the globe. The report abuse button can be used to report inappropriate or potentially illegal activity towards a child. It can be found in many websites, chatrooms and instant messaging services.

The IWF: www.iwf.org.uk

- The Internet Watch Foundation (IWF) is the UK hotline for reporting illegal online content – this may be child abuse images, or material considered to be criminally obscene or inciting hatred. A link for reporting illegal content appears on the IWF homepage.

ChildLine: www.childline.org.uk

- Children and young people can ring ChildLine on 0800 1111 to speak to someone in private. The ChildLine website also offers excellent help and advice on a whole range of issues, for example online safety, sexting, grooming and bullying.

Parent Port: www.parentport.org.uk

- ParentPort is run by the UK's media regulators who set and enforce standards across the media to protect children from inappropriate material. At ParentPort parents can find out about the standards expected from the media, make a complaint and share views.

- **Stop it Now!** www.stopitnow.org.uk
- Stop it Now! UK and Ireland is a child sexual abuse prevention campaign run by the Lucy Faithfull Foundation. It supports adults to play their part in prevention through providing sound information, educating members of the public and running a free phone confidential Helpline.

Marie Collins Foundation: www.mariecollinsfoundation.org.uk

- The Marie Collins Foundation (MCF) is a UK charity which aims to enable children who suffer sexual abuse and exploitation via internet and mobile technologies to recover and live safe, fulfilling lives.

Action Fraud: www.actionfraud.police.uk

- Action Fraud provides a central point of contact for information about fraud and financially motivated internet crime. Contact can also be made with Kent Trading Standards: www.kent.gov.uk/business/trading-standards/consumer-protection

How can I find out more about online safety?

Professionals should be encouraged to access appropriate online safety training to enable them to work confidentially with children, young people and parents/carers. Local training may be available via your own agency so professionals should contact their DSL for further information. Education settings within Kent can access support and training via the Education Safeguards Team.

The Kent Safeguarding Children board provides multi-agency training for professionals, both as e-Learning and via face to face sessions.

National training and resources are also available via a range of organisations. Please see references for further details, contact information and links.

What should I do if I am concerned about current online safety practice in my organisation?

If you believe there is evidence of misconduct by any member of your organisation then this should be reported to your designated safeguarding lead (DSL) and/or following your organisations whistle blowing policy and procedures.

DSLs may wish to consult with Kent County Council (via the LADO if there is an allegation being made against a member of the children's workforce), Personnel services, Social Services or the Police, if appropriate.

Frequently Asked Questions: Keeping Myself Safe Online

Please be aware that staff must always follow their organisations appropriate policies e.g. codes of conduct, acceptable use policies (AUPs), safeguarding report mechanisms etc.

Can my organisation limit my own private use of social media?

Your workplace cannot prevent you from having or using social media in your own personal time. However they can put in place appropriate boundaries and recommendations in order to safeguard you as well as the children, young people and families you work with.

Many professionals may be under the assumption that their personal use of social media is personal. However for professionals who are members of the wider children's workforce (including teachers, social workers, early year's staff etc.), it is essential to recognise that we are all role models, both on and offline. It is also important to be aware that once content is posted online it cannot be considered to be private as anyone who can see it, can copy and share it without your knowledge or consent.

One common situation may include a professional complaining about a parent's rudeness on their social media site. Had the conversation remained private as no-doubt was intended, this might be regarded as simply 'letting off steam'. However, if a social networking site was used with incorrect privacy settings (or indeed was copied and shared by anyone who has access to the content) then an unintended audience could be included and a formal complaint or allegation could be made.

This situation is not new; staff discussing children, young people or families in a shop queue might be overheard by a parent. However technology enables these conversations or messages to be copied, recorded, edited maliciously, used out of context, re-published or used as evidence.

The mode of use of social networking and instant messaging is often conversational with a rapid interchange of remarks. It is easy to stray from a non-work conversation between friends to professional matters which can be a breach of professional confidentiality.

Staff members should either be fully conversant with the security and privacy setting for the site in use or should avoid posting any information or content which could compromise their professional integrity.

Should I continue to use my own personal Social Networking site?

Social networking is an excellent way to share news with family and friends. Providing the security of your profile has been set correctly and a strong password used, information should remain private. The danger is that few people understand profile privacy settings. Social Networking is a way of life for many children, young people and adults. However adults working with children and young people should review their use of social networks as they take on professional responsibilities. Strong passwords should be used and security or privacy settings should be applied so that you can control all access to your profile.

Once published, information such as photographs, comments, blog posts etc. are almost impossible to control and could potentially be manipulated without your consent or knowledge, used in different contexts or further distributed. Some adults have been "caught out" by posting comments or remarks about work or colleagues only to find them re-published elsewhere. Even joining an online game or liking a post which contains offensive language (even as a "joke") could be misinterpreted.

False social networking sites have been set up by children, young people, parents/carers and even colleagues with false or malicious information about staff. Currently few social networking sites authenticate their members' offline and generally they use automated registration systems which can only provide limited checks. Some instant messaging applications have a facility to record a log of conversations which can be used to protect staff in case an allegation is made, however this records can be edited. It is essential that staff protect their professional reputation, both on and offline.

How can I keep my Social Networking use safe?

It is important that professionals are in control of their professional reputation online, even if they do not have a social networking account themselves. If professionals do not maintain their online identify then it is possible that information will be available online without your knowledge. It can be a good idea to undertake a search on your name using public search engines such as Google or Bing to help you to identify any publicly available content such as social media posts, websites or images. If you see anything which is concerning, then you should review your social media privacy settings, delete any inappropriate content, deactivate any old accounts or contact the relevant person or websites involved and request assistance in removing the content.

It is essential to review the content and privacy settings on any social network account(s) you have on a regular basis. Professionals should always carefully consider any photos posted online and think about who might be able to see, and therefore copy them. For example on Facebook your profile photo and cover photo are always public so it may be a wise idea to post photos which do not identify you or share any personal information, such as photos of your own children.

Most social networking sites have settings which enable you to control or limit who has access to the content which you share. Professionals should also be mindful of commenting on their friend's walls or on any public news stories etc. as this may be visible by others. It is recommended that all content shared online is limited to 'friends' only, however professionals must be aware that it is best to treat all information

posted online as being potentially permanent and public. The UK safer Internet Centre has helpful information about some popular websites and apps safety tools and privacy settings here: www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals/safety-features

Professionals should think carefully about whom they are friends with, and which friends can access what information online. It is a good idea for professionals to remove any "friends" who could compromise your professional role. However if there are pre-existing relationships (such as you are friends with parents socially, or work with a child/young person who is also a family member) then it is essential to discuss these situations with your organisations Designated Safeguarding Lead.

It is strongly recommended that professionals do not list their place of work on their social networking profile as this increases the risk of both being identified and potentially bringing your organisation into disrepute and this could lead to disciplinary action.

If you are approached or contacted by a child, young person or parents/carer online then you should decline the request and inform your Designated Safeguarding Lead and/or line manager as soon as possible.

If you wish to use social media professionally, for example use Twitter to take part in CPD events such as joining in discussion at a conference or event, then you might wish to consider creating a separate and distinct social media presence. This will ensure that professional boundaries are maintained and you are able to safeguarding both your personal and professional life. You should discuss your use of social media as a tool for your CPD with your line manager and ensure that you are aware of and following your organisations social media policy, code of conduct and Acceptable Use Policies at all times.

How can I protect my own personal devices?

Your organisation cannot ban you from having a personal phone, email address etc. but they can put in place expectations regarding safe behaviour within the workplace. This will be especially important if you work directly with children, young people and families. If it is provided, then it is a good idea to lock personal devices in a safe and secure place unless you are using them, for example lock your mobile phone in a draw or locker until your lunch break.

It is recommended that you ensure that any personal devices are suitably protected e.g. by setting a PIN, password or passcode to prevent accidental or deliberate misuse. Some professionals have had their reputation undermined or have put themselves, children, young people or parents at risk following clients accessing personal photos and details stored on devices which have then been made public. This may include accessing your personal details, such as where you live, using your device to access illegal or inappropriate content or accessing your personal photos.

Professionals should ensure that passcodes, passwords and PINs are strong and secure and use a mixture of lower and upper case letters, symbols and numbers. These codes should not be shared with others or written down and should be changed regularly. You should avoid dictionary words or number sequences e.g. password, 1234 etc. as they are easy to guess. It is recommended that different passwords are used on

different systems so if one account is compromised, others will still be secure. Using strong PINs, passwords and codes will help prevent other people from accessing your accounts and can helps to prevent identity theft.
Staff should also be aware that for some devices, information and apps may still be accessed even if a phone is locked and should ensure that appropriate settings are applied to their device to restrict this. For example iPhones can allow users to take photos on the device even when the screen is locked.

It is good practice to make sure you logout of any social media apps or systems following use as this will prevent people posting content or accessing private information.

Useful advice on setting safe and strong passwords can be found here:

- www.google.com/safetycenter/everyone/start/password
- www.getsafeonline.org/protecting-yourself/passwords
- www.connectsafely.org/tips-to-create-and-manage-strong-passwords

How can I use technology appropriately to communicate with children and young people?

Young people are encouraged to report concerns, and this may involve the use of new technology, e.g. a young person might prefer to text a report about bullying, rather than arrange a face to face discussion or may prefer you arrange an appointment to see them by text rather than by letter.

Friendly verbal banter between adult and child/young people may not be inappropriate, but it might look very different if carried out via email or social media and might lead to difficulties if misinterpreted, forwarded or used out of context. Care in the use of appropriate electronic signatures or any usernames etc. selected is required when communicating within in a professional setting. Adults should be aware of, and comply with, the organisation policy on the use of text or social media and be circumspect in their communications with children and young people so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming.

Professionals should never use their personal email address, home address or phone line (fixed or mobile) to communicate with children, young people or clients. In all situations any sudden or urgent communication must be approved by the DSL or line manager. In all cases ensure that your relationships with children, young people are known, approved and recorded by the DLS and your line manager.

Should I have children and young people as my ‘friends’ on social media or other services?

In some circumstances, such as education and youth work, online communication via social media can provide excellent opportunities for collaborative work between professionals and children, and when appropriately arranged, can guide and enhance such activities.

Communication between adults and children/young people, by whatever method, must always take place within clear and explicit professional boundaries. Professionals should not share any personal information with children or young people. Staff should not request, or respond to, any personal information from the child / young person, other than that which might be appropriate as part of their professional role and in accordance with their agencies codes of conduct. Professionals should ensure that all communications are transparent and open to scrutiny.

It is strongly recommended that professionals do not add children, young people or their parents/carers as ‘friends’ on any personal social media services. By accepting children, young people or parents as ‘friends’ on your social media sites, could mean that you are vulnerable as you will be sharing personal information or having access to personal information about your children and families. You may be potentially leaving yourself open to allegations of inappropriate contact or conduct or even find yourself exposed to unwanted contact. Your organisation should provide guidance regarding this in their Code of Conduct or Acceptable Use Policy (AUP).

Any pre-existing relationships or exceptions between children or parents which may compromise this (for example your own children are pupils at the school you work are or a parent is a family member or friend) must be discussed with your organisations DSL and/or manager. This will help to ensure that the relationship is formally acknowledged and will enable your DSL/ manager to discuss with you your organisations expectations regarding professional conduct.

Consideration should always be given as to how this type of communication might appear to a third party. Compared with a conversation within a formal workplace environment e.g. within a school, the use of technology inevitably increases the potential for messages to be seen out of context or misinterpreted.

Personal e-mail addresses, instant messaging identities, social networking accounts or telephones (fixed or mobile) should never be used to contact children or young people or parents/carers. A separate professional account or contact should be used, with the agreement of management, following an appropriate risk assessment and the decision MUST be formally recorded

Professionals should use an online environment which is under their control. The first requirement is that you know who you are talking to; users must be authenticated. An official provided communication and collaboration area will have a range of security features set within a policy framework. Logs should be available in case a false allegation is made.

Should I use my personal mobile phone or device to take photographs or videos of children and young people?

It is important to continue to celebrate achievements of children and young people through the appropriate use of photography in communicating with parents and the community. A school trip is a common situation where photography by children and staff should be encouraged, but there are potential dangers.

The safest approach is to avoid the use of personal equipment and to use an organisation or agency provided item. One potential danger is an allegation that an adult has taken an inappropriate photograph. With a personal camera it would be more difficult for the adult to prove that this was not the case. With organisation equipment there is at least a demonstration that the photography was consistent with organisations policy. Use of personal devices to take photos or videos can also potentially undermine the wider safeguarding culture within a setting.

Staff should always ensure they have appropriate consent to take photographs and videos to ensure compliance with the Data Protection Act. Organisations must have written parental consent to take, store and use images of children. Care must also be taken that photographs are stored appropriately and in accordance with the law. For instance to copy the photograph on to a personal laptop as opposed to a work allocated laptop might make it difficult to retain control of how the picture is used. Work provided, secure and encrypted memory cards, USB memory sticks and CD's should only provide a temporary storage medium. Once photographs are uploaded to the appropriate area of the work network, images should be erased immediately from their initial storage location. If a personal device is uses then this could breach data protection legislation.

If personal devices are used in emergency circumstances then this practice should be discussed with and approved by your DSL and you must follow data protection legislation and ensure that children and staff are appropriately safeguarded. Any images taken of children and young people must not be shared or posted on any staff personal social networking accounts and should be shared by official and approved social media channels only. The decision regarding this approach should be clearly and formally risk assessed and documented and explicitly monitored by the DSL within your organisation.

Specific guidance for education settings is provided within the "Image Use Policy" 2016 available on Kelsi: www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding/e-safety

Someone has posted comments about me on a social media site – how can I get them removed?

This is a difficult issue to respond to and sadly it isn't always possible to prevent people posting comments online about us. Children, young people and parents are entitled to hold opinions about us and our organisations, many of which may be positive, some might not be so pleasant and expressing these views is not always illegal. However this does not mean that this behaviour should be tolerated, especially if it is directed at specific individuals. Unless the comments make a credible threat to safety (e.g. threats of violence), name a teacher who is subject to an allegation and who is yet to be charged (this is specific to teachers), contains hate content, could be considered as harassment (and therefore a criminal offence has been committed) or breach the sites terms and conditions, then comments posted online cannot always be forcibly removed. The best course of action is to adopt a partnership approach and for DSLs and leaders to speak directly with any members of the community involved when any concerns are raised.

If you are the victim of cyberbullying or harassment by a child, colleague or parents/carer, for example, a parent makes inappropriate comments about you, then don't retaliate and make sure that you save and print any evidence such as wall posts, URLs, messages, comments, names, times, dates and locations etc. You should then report your concerns to your DSL and/or manager. Employers have a statutory duty of care for the health, safety and welfare of staff and should therefore take reasonable steps to support staff experiencing cyberbullying or online harassment.

You may wish to access support for yourself, such as via any professional unions. The UK Safer Internet Centre provides a helpline for professionals working with children and young people in the UK with any online safety issues they may face themselves or with children in their care. The Helpline aims to resolve issues professionals face about themselves, such as protecting professional identity and reputation, as well as young people in relation to online safety. www.saferinternet.org.uk/about/helpline

Frequently Asked Questions: Keeping Data and Systems Safe

Please be aware that staff must always follow their organisations appropriate policies e.g. codes of conduct, acceptable use policies (AUPs), safeguarding report mechanisms etc.

How should I store personal data safely?

Professionals working with children and young people often find it convenient to work at home writing reports, assessments etc. This may require access to confidential personal information including images of children.

The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights let individuals find out what information is held about them. The eight principles are that personal data must be:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than is necessary
- Processed in line with individual's rights
- Kept secure
- Transferred only to other countries with suitable security measures.

All personal information, including images, must be kept secure at all times. The storage of data on a hard disk or memory stick and transfer by email or other means is basically insecure. Making such storage secure may include password protection, encryption of data and locking the computer when not in use. Risks including mislaying a memory stick, mistyping an email address, saving confidential files on a shared computer (such as a family laptop which children or other family members have access to) and laptop theft from a vehicle are all too common. Professionals should consider approaches such as not storing information unless necessary and always deleting files (not just placing them in the recycle bin) after use.

The safest long-term storage location may be the work network, which should have a remote backup facility. Information security is an integral part of the Data Protection Act 1998. You must take all reasonable steps to ensure that any personal information that you are processing is securely stored. Please refer to your organisation's policy or the KCC guidance available.

Professionals must also take care to prevent others gaining access to your information accessible via your work account, particularly when using work mobile phones and laptops in areas where children, families or members of the public may have access to them. You should never leave your computer or work device unsupervised or unlocked while you are logged in or allow someone else to access it. Professionals should always lock their computer screens or use pin/passwords to protect them when they are not in use and should always log out of systems and accounts when they have finished using them.

All professionals are strongly advised to ensure that they understand the organisation policy regarding data protection. This may also be highlighted within other documents such as your organisations Acceptable Use Policy (AUP). National policy is developing rapidly in this area. To lose control of personal data while not complying with the policy would be difficult to defend.

Can I use online cloud systems to store data or images for work?

Any use of cloud storage must be in accordance with your organisations data protection and information security policies and therefore in accordance with the Data Protection Act (DPA) 1998.

Any files (paper or electronic), containing personal data must always be stored in accordance to the Data Protection Act and this is a legal requirement as part of organisations obligations as a data controller. Using a cloud computing service does not change these legal duties with regards to Data Protection, Freedom of Information etc. and the organisation must ensure that it is compliant with the legislation and that the setting can meet its statutory safeguarding responsibilities.

Professionals should be aware that cloud computing may not be appropriate for all uses, especially where security of confidential data and personal data is involved and should not be used unless it fully meets DPA requirements and is suitably encrypted. Some services e.g. Google Drive, Dropbox, iCloud etc. do not always store data within the EU (they may have signed up to safe harbor agreements but this may not always be sufficient) so it would not be advisable to use cloud storage hosted outside of the EU to store any content or files which would be considered confidential or which may be subject to the DPA e.g. contains personal information.

Professionals should only use organisational provided and appropriately risk assessed systems to store any work data or images.

If in any doubt as to if a system is safe to use to store data and images then professionals should speak to their DSL and information governance lead.

What is my responsibility for the use of my work laptop or device at home?

Personal use of technology by adults has been shown to increase competence and confidence and should therefore be encouraged. However work devices provided by organisations for professional practice are always the property of your organisation and are intended for professional use only.

Things that can go wrong include:

- Access to wider sites by family members, for instance a gaming site or internet shopping, would increase the possibility of virus attack and identity theft.
- If another member of the family or a friend is allowed to use the computer it is difficult to ensure that the use has been appropriate, for instance that confidential information has not been accessed. Adults vary enormously in their judgements as to what is appropriate.
- If a work laptop is used at home for personal use, then it may be a taxable benefit.
- Some professionals may feel that access via a work laptop to adult material outside working hours and at home is appropriate. It is not; there is always a possibility that this material might be accidentally seen by a child or young person and in some cases this type of use has led to dismissal.
- Professionals need to remember that in order for anyone else to use a work laptop in the home setting, they would need to be logged on by the person responsible for the laptop. With this in mind, misuse of that laptop is likely to rest with the designated user of the laptop.

Professionals should refer to the organisations policy on the personal use of work laptops, which unfortunately varies between organisations and between local authorities. Increasingly the use of a work computer for non-professional use is being explicitly banned. Professionals should always ensure that they have absolute control of a work devices allocated to their use. This issue may also be highlighted within other documents such as your organisations Acceptable Use Policy (AUP).

As a technician, how can I safely monitor my schools network use?

Filtering or recording network usage will only be effective if monitored carefully to notice and report inappropriate access or usage. Often this places a new responsibility on technical staff that they may not have been trained for. This responsibility can become onerous if a pupil or staff member is apparently implicated in inappropriate or illegal activity.

It is wrong to assume that filtering and monitoring are simply technical ICT activities, solely managed by the network staff. Some technical staff may have indeed taken on this wider responsibility to help ensure that ICT use is appropriate and beneficial. However technical staff should not be expected to make judgements as to what is inappropriate material or behaviour, without support and supervision. Technical staff must work together with schools DSL and managers to ensure the safety of all members of the community.

A technician might, with the best of intent, check sites that a user has visited and email images to alert a colleague to a safeguarding concern. Should the images prove to be illegal the technician has potentially committed a criminal offence. A defence may be that the technician was acting within a published school procedure, but staff should ensure that they receive a specific, written request to perform this work. Should any incidents of concern occur, then there should be a clear route for immediate reporting to the DSL. Procedures to preserve evidence by unplugging a computer or locking an account need to be in place.

The filtering and monitoring policy must be set by DSL and leaders, with set procedures to deal with incidents. Leaders must ensure that members of technical staff are supported in their role in maintaining the ability to monitor the network when making purchasing decisions. For example if a school leader buys a set of class tablets, the technical staff should be involved to ensure that devices are compatible with current systems or can be managed in accordance with the schools legal safeguarding requirements as outlined within the Prevent Duty and Keeping Children Safe in Education 2016.

A common concern found in these situations is that non-technical staff may not be aware that without an identifiable user (e.g. login details) it may not be possible to identify and trace misuse of the network and systems. For example if users do not have to login to use tablets whilst on the school network and it was discovered that a user was accessing indecent images of children or extremist content then it would be difficult and in some cases impossible to work out who was responsible. This could mean that leaders are not complying with their statutory safeguarding responsibilities and could ultimately place children at risk of significant harm.

Further advice regarding appropriate monitoring and filtering can be found via the UK Safer Internet Centre here: www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals/appropriate-filtering-and-monitoring

Schools may also wish to contact their broadband provider directly for further advice and information.

Useful Links and Resources

Kent Links

Guidance and policy template for Education settings regarding “Image Use”: www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding/e-safety

Kent educational settings online safety policy template and guidance 2016: www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding/e-safety

Kent information governance: www.kelsi.org.uk/school-management/data-and-reporting (KCC staff should also access KNet for further information)

Kent Safeguarding Children Board: www.kscb.org.uk

Kent Police: www.kent.police.uk/internetsafety

National Links

Guidance for Safer Working practice for Adults who work with Children and Young People: www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding/safeguarding-policies-and-guidance

National Education Network: www.nen.gov.uk

Childnet: www.childnet.com

UK Safer Internet Centre: www.saferinternet.org.uk

Internet Matters: www.internetmatters.org

Think U Know: www.thinkuknow.co.uk

NSPCC: www.nspcc.org.uk/onlinesafety

Acknowledgements

This document is the work of the Rebecca Avery, Education Safeguarding Adviser (Online Protection) and the Kent e-Safety Strategy Group on behalf of the Kent Safeguarding Children Board (KSCB).

Additional material has been used and developed with thanks to the following organisations:

South West Grid for Learning
Childnet
UK Safer Internet Centre
CEOP Education Team

Safer Professional Practice with Technology

September 2016