Kent Safeguarding Children
multi-agency partnership

Medway
Safeguarding
Children Partnership
Safeguarding Medway's
children together

Kent and Medway Safer Professional Practice with Technology: Frequently Asked Questions

April 2023

Document Author	Kent Safeguarding Children Multi-Agency Partnership (KSCMP) Medway Safeguarding Children Partnership (MSCP)
Document Owner	**Kent Safeguarding Children Multi-Agency Partnership** Sessions House Maidstone ME14 1XQ Email: kscmp@kent.gov.uk **Medway Safeguarding Children Partnership** Gun Wharf Dock Road Chatham ME4 4TR Email: mscp@medway..gov.uk
Summary of Purpose	The Kent Safeguarding Children Multi-Agency Partnership (KSCMP) and Medway Safeguarding Children Partnership (MSCP) have developed this frequently asked questions guidance to help professionals working with children, young people and their families to ensure that their use of technology is safe and appropriate.
Accessibility	This document can be made available in large print, or in electronic format. There are no copies currently available in other languages.
Equalities Impact Assessment	During the preparation of this policy and when considering the roles and responsibilities of all agencies, organisations and staff involved, care has been taken to promote fairness, equality, and diversity, in the services delivered regardless of disability, ethnic origin, race, gender, age, religious beliefs or sexual orientation.
Copyright ©	Copyright Kent Safeguarding Children Multi-Agency Partnership and Medway Safeguarding Children Partnership. All rights reserved including the right of reproduction in whole or in part in any form or by any means without the written permission of the author/owner.
Policy Review Date	This document will be reviewed in April 2026, as a minimum.

Contents

1. **Introduction**

About this document 5
Aims of the document 6
Suggestions for use 7
Questions for further discussion 7

2. **Frequently Asked Questions: Keeping Children and Young People Safe Online**

What risks should I be aware of online? 8
What is classed as 'inappropriate'? 9
How do I ensure safer online activity when working directly with children and young people? 11
I'm working with a family who want help to keep their children safe online, what resources are available to help them? 12
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? 13
I'm aware that a child or young person is playing 18 rated video games, should I tell the police? 14
Somone I'm supporting is sharing or accessing content online about self-harm, suicide or eating disorders – how should I respond? 16
I'm concerned someone may be at risk of domestic abuse through technology use – is there support available? 17
I'm aware of someone under the age of 18 has taken or received nude or semi-nude photos of another person under the age of 18 – should I just tell them to delete it? 17
Someone I'm supporting is sharing or accessing misinformation or disinformation online – how should I respond? 19
I have heard about a harmful or distressing challenge/content circulating online. I'm not sure if it's true or not but how should I respond? 19
How can I recognise if the time someone is spending online is harmful to them? 20
I think someone is at risk of cybercrime – how can I support them? 21
Someone has told me that they are being bullied or harassed online – what advice can I give them? 22
What should I do if a child or young person discloses online abuse or exploitation? 23
I'm working with a child, young person, or family who have experienced a specific concern online – what support is available for them? 24
How can I find out more about online safety? 25
What should I do if I am concerned about current online safety practices in my organisation? 26

3. **Frequently Asked Questions: Keeping Myself Safe Online**

Can my organisation limit my private use of social media? 27

Should I continue to use my own personal social networking sites? 27
How can I keep my social networking use safe? 28
How can I protect my own personal devices? 29
How can I use technology appropriately to communicate with children, young people and families I support? 30
Should I have children, young people and/or adults I support as 'friends' or contacts on my personal social media account or other services? 30
Should I use my personal mobile phone or device to take photographs or videos of clients? 31
Somone has posted comments about me on a social media site – how can I get them removed? 32
I'm concerned about the online behaviour of a colleague – what should I do? 33
I've seen something harmful or hateful online – what should I do? 34

4. Frequently Asked Questions: Keeping Data and Systems Safe
How should I store personal data safely? 35
Could I use online cloud systems to store data or images for work? 36
What is my responsibility for the use of my work laptop or other devices at home? 36
As a technician, how can I safely monitor my organisations network use? 37

5. Useful links and Resources 39

1. Introduction

Online safety, online safeguarding, or e-Safety (as it used to be called) covers issues relating to children, young people and adults, and their safe use of the internet, mobile phones, tablets and other communication technologies and devices, including wearable and smart technology, in a range of settings including schools, early years providers, local sport clubs, youth groups, 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.

It is important to recognise that children may be harmed by people and in spaces outside of their home, this is also known as extrafamilial harm. Dr Carlene Firmin uses the term 'contextual safeguarding' to describe how the places themselves, such as school, parks and online spaces can increase a young person's risk of being harmed. Dr Carlene Firmin's research shows that professionals often fail to correctly engage with, or assess, the risk of these spaces. Online spaces, unlike schools or neighbourhoods, can be hidden from parents, teachers, and other professionals or adults and so provide opportunities for children and young people to be exploited and abused without being detected. In the modern world of smartphones, online spaces are also mobile and a constant presence for young people. This places an emphasis on the adults working with young people to know what sites they are accessing, what content they are reading/watching and who they are speaking to.

About this document

The Kent Safeguarding Children Multi-Agency Partnership (KSCMP) and Medway Safeguarding Children Partnership (MSCP), have developed this frequently asked questions guidance to help professionals working with children and young people 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, health, and libraries. 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 should ensure that the content is suitably adapted or amended to meet any specific organisational needs or expectations.

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

A simplistic rules-based approach will not resolve complex issues, but local and national legislation and guidance, including the KSCMP and MSCP 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.

For schools, early years providers and other education settings, the Education Safeguarding Service act as the agency lead for education and provide specialist advice and support regarding online safety.

Aims of the document

This document aims to explore several frequently asked questions to:

- Ensure safeguarding children and young people online is a priority
- Assist professionals to work safely and responsibly and to monitor their own standards and practice
- Help professionals 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 professionals about inappropriate online 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 clients online within their organisation.

Managers and agency leads for safeguarding (often known as Designated Safeguarding Leads or DSLs) should ensure they are clear about the specific expectations regarding what their organisation considers to be safe and appropriate use of technology, and should 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.

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
- Abide by any relevant professional standards or expectations
- 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 and/or emerging risks or trends.

Suggestions for use

This document covers a variety of topics, and it may not be appropriate or necessary to share it in full with all staff. It is recommended that leaders and managers consider using this document via a range of approaches, as appropriate to their staff, to ensure they are aware of the relevant issues and their implications.

Possible options to consider are:

- Clear references within existing organisational policies/procedures/guidance on the safe and appropriate use of technology
- Providing sections, copies of or links to this document to members of staff as part of induction
- Place copies of or links to this document in staff areas, for example, the staff room, intranet systems
- Providing extracts, copies of or links to this document to 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
- Using some of the statements within staff induction, staff development or training sessions, and discussing some of the issues and implications highlighted
- Using relevant content to inform and develop their own internal policies and procedures

Questions for further discussion

The following questions might also be useful for Designated Safeguarding Leads (DSLs) to initiate further staff discussion:

- Can I use a work device 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/carers, or other professionals?
- Can I use my personal phone 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 phone 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, for example, for my own CPD?

2. Frequently Asked Questions: Keeping Children and Young People Safe Online

Please be aware that staff should always follow their organisations appropriate policies, for example, codes of conduct, acceptable use policies, and safeguarding reporting mechanisms.

What risks should I be aware of online?

In today's modern society, children and young people 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 internet users in danger. Professionals need to acknowledge the role and influence of technology when working with children and young people 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
- **Commerce:** being at risk of financial harm

These issues can be summarised as:

	Commercial	**Aggressive**	**Sexual**	**Values**
Content Child/adult as recipient	Advertising Spam Copyright Sponsorship Hacking Fraud/Scams	Violent content Hateful content	Pornographic content Unwelcome sexual comments/ harassment Receiving nude or semi-nude images from peers Revenge pornography	Bias Racist and extremist content Misleading info/advice Body image and self-esteem Distressing or offensive content Neglect
Contact Child/adult as participant	Tracking Harvesting data Sharing personal information	Being bullied, harassed, or stalked	Online dating scams Sexualised bullying and harassment Grooming Online child sexual exploitation	Self-harm, pro-eating disorder and suicide content Grooming for extremism and radicalisation

			Taking nude or semi-nude images	
Conduct Child/adult as actor	Illegal downloading Hacking Gambling Privacy Copyright	Bullying, harassing or stalking others	Creating and uploading inappropriate or illegal sexual content (including sharing nude and semi-nude images of themselves or others) Unhealthy or inappropriate sexual relationships or behaviour Child on child sexually 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 2018

It is important professionals recognise that online abuse can be perpetrated by children, young people and adults towards their peers, as well as by family members and strangers.

Online safety is an increasingly common feature in safeguarding practice/case reviews and domestic homicide reviews, so it's important all professionals are aware of the risks and how they can support the children and young people they work with.

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 accessing illegal content may lead to a criminal investigation and prosecution. Where members of staff are involved, this can lead to disciplinary action, dismissal, and barring, even if there is no criminal prosecution.

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

Illegal:

- Accessing (viewing), making, storing (possessing) or disseminating indecent images of children on or off the internet, is illegal (Protection of Children Act 1978, Section 1.1a, and Criminal Justice Act 1988, Section 16). Possessing or distributing indecent 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 images.

    - This offence also applies to indecent images created by children and young people (those aged under 18) themselves and is often referred to as sharing nudes or semi-nudes, youth produced/involved sexual imagery or 'sexting'. Children and young people may have created images as part of age-appropriate sexual development, however in some cases, they may have been harmed or coerced into posing for such images and will therefore be victims of child sexual abuse and exploitation. National advice for educational settings is available via the UKCIS 'Sharing nudes and semi-nudes: advice for education settings working with children and young people' and local guidance for professionals regarding responding to nude or semi-nude image sharing can be found on the KSCMP and MSCP website.
    - Staff should 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 organisations child protection policy) and police advice should be sought urgently via 101 or 999 if there is an immediate risk of harm.
- Causing a child to watch a sexual act, for example sharing pornography with children (under 16) for the purpose of obtaining sexual gratification is illegal (Sexual Offences Act 2003, Section 12).
- The offence of grooming is committed if someone over 18 has communicated with a child under 16, on one or more occasions (including by phone or using the internet) and intentionally 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).
- The Serious Crime Act 2015 (Part 5, Section 67) makes it a criminal offence for an adult (person aged over 18) to send a child (under 16) sexualised communications or sends communications intended to elicit sexual communications. The offence is committed whether or not the child communicates with the adult.
- Section 69 of the Serious Crime Act 2015 also makes it an offence to be in possession of paedophile manuals, information, or guides (physically or electronically) which provide advice or guidance on sexually abusing children.
- Section 33 of the Criminal Justice and Courts Bill 2015 makes it an offence to share private, sexual materials, either photos or videos, of another person without their consent and with the purpose of causing embarrassment or distress; this is often referred to as 'revenge porn'. The Domestic Abuse Act 2021 extended this to cover the threat of disclosing photographs.

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. It is an offence to make credible threats or send offensive messages with

the purpose of causing the recipient distress or anxiety. This can include for example, cyberbullying by mobile phone and/or social networking sites.

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
- Children, young people and professionals being sent racist or homophobic comments
- Staff forming sexual relationships with children or young people

Inappropriate:

Think about inappropriate content and behaviour 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 you and may constitute gross misconduct.

Examples taken from real events:

- Posting offensive, derogatory, or insulting comments about the colleagues, clients, 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 or internet connections during break
- Liking or sharing extremist views or content on social networking sites
- Using personal devices for personal use (for example, 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 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 and young people. However, there is always an element of risk; even an innocent search can occasionally turn up links to adult content and imagery. Professionals working within the community, such as within family or service users’ homes, should be aware that filtering may not always be in place so additional degrees of caution will be required.

Planning and preparation are vital and the safest approach when using online material is to always check sites and services before use. Be aware that the internet is dynamic and content perceived as ‘safe’ today might not be as ‘safe’ tomorrow.

You should carefully consider the age, ability and maturity of service users when planning online activities. When working with 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 or vulnerable adults, consideration should be given to staff selecting appropriate and safe search engines and/or ensuring safe search settings are in place. However, you should be aware that this only reduces and doesn't remove the risk of accessing unsuitable content, especially when searching for images or videos. Appropriate search terms should be used and pre-checked where possible.

When encouraging service users to publish work or engage with others online, you should ensure that age and ability appropriate sites and services are used. If you are using online video clips with children, young people, or adults you are supporting, you should 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 staff should turn off the monitor/screen, reassure the children/young person/adult and to protect, log and report the URL in line with your organisations policy, for example, to a member of senior staff. Professionals should avoid printing or capturing any inappropriate material and should not print, forward or save illegal content.

I'm working with a family who want 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. A significant amount of internet access takes place when children and young people are within the home therefore it is essential that families are aware of children's internet use and implement appropriate measures to safeguard them online.

Technology can sometimes be seen as 'scary' or 'frightening' for many parents as they may be concerned about not having sufficient IT skills to help protect their child. This fear can prevent them from taking appropriate measures to safeguarding their children, which unlimited, puts them at risk of harm. The important part of online safety is 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' or 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.safeinternet.org.uk
- www.childnet.com

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

If parents/carers request help for specific concerns, consult with your agency lead for online safety and/or safeguarding as they 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 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. Most popular social networking sites (such as Facebook, YouTube, Twitter, Instagram and TikTok) therefore have an age restriction of at least 13+ - some are older, for example Whats App is 16+. You can find the specific age restriction for services by accessing their terms and conditions.

It is currently 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 but does break the platforms terms and conditions.

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, we run the risk of driving any problems or incidents such as abuse or bullying underground, which can be more dangerous than the use of social networking in the first place. Whilst professionals must be careful not to encourage or promote the underage use of social media, we need to recognise that children, young people and their parents/carers may need further information and support to make informed and appropriate choices.

Research commissioned by Ofcom and carried out by Revealing Reality found that providing a false age was only one of many potential triggers for experiencing online risks. The study found that a range of risk factors were identified which potentially made children more vulnerable to online harm, especially when these factors appear to coincide or frequently co-occur with the harm experienced. These include:

- a child's pre-existing vulnerabilities such as any special educational needs or disabilities (SEND), existing mental health conditions and social isolation

- offline circumstances such as bullying or peer pressure, feelings such as low self-esteem or poor body image
- design features of platforms which either encouraged and enabled children to build large networks of people – often that they didn't know; or exposed them to content and connections they hadn't proactively sought out; and
- exposure to personally relevant, targeted, or peer-produced content, and material that was appealing as it was perceived as a solution to a problem or insecurity.

The study found that the severity of the impact of risk varies between children and ranges from minimal transient emotional upset (such as confusion or anger), temporary behaviour-change or deep emotional impact (such as physical aggression or short-term food restriction), to far-reaching, severe psychological and physical harm (such as social withdrawal or acts of self-harm). Adults should therefore ensure that 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, rather than solely focusing on underage use of social media as the main risk.

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 sexualised content, then you consider if they and/or their family requires specific intervention or support. Consider sharing your concerns about the child's use of social media with their parents/carers and see if they can understand the concern you have relating to their child's behaviour and discuss appropriate actions they can take to safeguard their child.

If parents/carers fail or refuse to protect their child online once a concern has been raised with them, you will need to respond in line with local procedures and explore other agency involvement, for example by making a referral to adult or children's services via existing local procedures and mechanisms. This is more likely to be the case for younger children or if there has been a serious incident linked directly to their use of social media. In these situations, professionals should always follow their organisations safeguarding policies and procedures and should speak to their DSL immediately if they believe a referral is required. Education settings can seek specific advice from the Education Safeguarding Service.

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 shops 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 consider the impact you may be seeing on the child, focus on raising parents' awareness about the possible risks, and education for the whole family about reporting concerns and understanding appropriate on and offline conduct.

PEGI provides age classifications for video games and will help parents make informed decisions about the suitability of games they allow their children to play. The PEGI rating of a game is based on two different levels; the age suitability (not difficulty) such as 3+, 18+ and content indications, which explore possible harmful content, for example violence or sexual themes.

The impact of video games, especially for children and young people, is widely debated and research is often inconclusive or conflicted. Some studies suggest that the impact of playing video games may depend on the individual, for example if they are already pre-disposed to aggressive behaviour and suggests that there is often a range of other factors involved, including family environment, age, and ability. Awareness and education about the potential impact is usually the best solution. In many cases, it will be beneficial to discuss the impact of a game on someone's behaviour, rather than just thinking about age ratings and helping children and adults make informed decisions.

In some cases, there may be no concerns regarding the content of the game being played, however serious safeguarding risks could still be encountered; this is often because many popular games contain an online element where players can talk with other people, or because their interest in a particular game may have led to them to access alternative platforms which offer video streaming and/or chat to discuss or watch others playing games.

Useful link 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.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 or online content linked to gaming, such as they are displaying violent, aggressive or sexualised behaviour or sharing potential extreme or hateful views, you should consider if the child and family or the adult requires specific intervention. Unless to do so would place a child at risk, you should consider sharing your concerns about children's use of gaming with their parents/carers first and see if they can understand your concerns and explore if they can/will 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, you will need to consider if other agencies need to be involved using existing local child protection procedures. 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, you should always follow your organisations safeguarding policies and procedures and should speak to your agency safeguarding lead immediately if you believe a referral is required. Education settings can seek specific advice from the Education Safeguarding Service.

Someone I'm supporting is sharing or accessing content online about self-harm, suicide or eating disorders – how should I respond?

The internet can be an incredible source of support for many children, young people and adults who are struggling to cope. It can allow them to access information and chat to other people who may be experiencing the same thing. However, online platforms can also provide them with opportunities to view upsetting and graphic content that could cause harm, including pro-eating disorder and pro-suicide and self-harm. Content like this can be viewed on most online platforms including social media, video sharing platforms and dedicated websites. It can be shared further on online forums, message boards and groups that have been set-up for people experiencing similar feelings.

Content that is harmful to one person might not be to another, and this can also depend on how someone is feeling in the moment that they see it. If someone is already experiencing low self-esteem or worrying thoughts relating to body image or mental health, then coming across more extreme content could negatively impact them without them realising. It can also be searched for using key words associated with the topic and hashtags.

It can be hard to recognise when something could be having a negative impact on our behaviour. Viewing these types of content online and hearing other people's experiences can make people feel less alone, but for some people it can make them feel worse, and it's important that they know how to seek support.

It can be upsetting for professionals and family members to discover someone is accessing content about suicide, self-harm or eating disorders. However, it's important to stay calm and to talk openly to them about it, without showing judgement or blame. It is also important to signpost them to specialist support and to always follow your agency safeguarding procedures if you feel the content poses a risk of harm.

Useful websites with further information and support for children and young people regarding eating disorders, suicide and self-harm include:

- Live Well Kent - free mental health support for people aged 17+
- Beat - support for young people and adults experiencing eating problems
- Childline – advice and support for children and young people
- Ripple Suicide Prevention Tool - a free browser extension that signposts people who have searched for suicide or self-harm content to mental health support and advice
- The Samaritans
- Mind
- Young Minds
- Shout
- Calm
- Rethink Mental Illness
- We are with you
- Mind and Body in Kent

- Internet Matters: Digital self-harm – is it a cry for help?

I'm concerned someone may be at risk of domestic abuse through technology use – is there support available?

The Domestic Abuse Act 2021 created a statutory definition of domestic abuse, emphasising that domestic abuse is not just physical violence, but can also be emotional, controlling or coercive, and economic abuse; it's important to recognise that this can take place online or be facilitated via the use of technology.

Technology and social media should be open and safe for everyone to use. Sadly, research has identified that perpetrators of domestic abuse are increasingly using online tools to abuse their victims. Technology can provide a positive place for victims to seek support, but it can also facilitate control and abuse; for example, partners reading emails, checking texts and social media posts, withholding or controlling access to online banking apps, sharing or threatening to share intimate photos, using tracking software to locate/track physical location or online activity and/or using social media to make threats. The Protection from Harassment Act 1997 also specifically addresses cyberstalking.

The following websites provide support regarding online risks and advice where technology can facilitate domestic abuse:

- Women's Aid: Online Safety
- Refuge: Technology Abuse
- Safe Lives: Digital and online safety advice
- Kent Police: Digital domestic abuse

If you are supporting someone who is experiencing domestic abuse, please follow your agency safeguarding procedures. Additional advice and support, locally and nationally can be accessed via:

- Domestic Abuse Services in Kent & Medway
- National Domestic Abuse Helpline
- Kent Police Domestic Abuse Support and Advice
- Revenge Porn Helpline
- National Stalking Helpline
- Bright Sky app
- Gov.UK: Domestic abuse: how to get help

I'm aware of someone under the age of 18 has taken or received nude or semi-nude photos of another person under the age of 18 – should I just tell them to delete it?

No; whilst it's possible that, depending on the context and the age and understanding of the young people involved, no further action will be required beside advice and support to the children and young people involved, it is also possible that the police and/or children's social care may need to be informed urgently. Only once a decision has been made by the organisations safeguarding lead that statutory agencies do not need to be involved, should nude and semi-nude images be deleted to limit any further sharing.

Nude and semi-nude image sharing is defined as the sending or posting of nude or semi-nude images, videos or live streams online by young people under the age of 18. This could be via social media, gaming platforms, chat apps or forums. Many professionals refer to ‘nudes and semi-nudes’ as youth produced/involved sexual imagery, indecent imagery (the legal term used to define nude or semi-nude images and videos of children and young people under the age of 18), ‘sexting’ or image-based sexual abuse. Alternative terms used by children and young people may include ‘dick pics’ or ‘pics’.

Creating and sharing nudes and semi-nudes of under 18’s (including those created and shared with consent) is illegal which makes responding to incidents involving children and young people complex, so it is essential prompt and appropriate safeguarding action is taken. The motivations for taking and sharing nude and semi-nude images, videos and live streams however are not always sexually or criminally motivated, so a balanced and proportional response is required.

If an incident comes to your attention:

- Report it to your agency designated safeguarding lead or equivalent immediately. Your setting’s child protection policy should outline codes of practice to be followed.
- Never view, copy, print, share, store or save the imagery yourself, or ask a child to share or download it – this is illegal.
- If you have already viewed the imagery by accident (for example, if a young person has showed it to you before you could ask them not to), report this to your agency designated safeguarding lead (or equivalent) and seek support.
- Do not delete the imagery or ask the young person to delete it.
- Do not ask the child/children or young person(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of your agency designated safeguarding lead (or equivalent).
- Do not share information about the incident with other members of staff, the young person(s) it involves or their, or other, parents/carers.
- Do not say or do anything to blame or shame any young people involved.
- Do explain to them that you need to report it and reassure them that they will receive support and help from your agency designated safeguarding lead (or equivalent).

Education settings should follow the UKCIS ‘Sharing nude and semi-nudes: advice for education settings working with children and young people’ guidance and can seek specific advice from the Education Safeguarding Service.

This advice does not apply to adults sharing indecent images of children (under 18’s). This is child sexual abuse and must be referred to the police as a matter of urgency.

Someone I'm supporting is sharing or accessing misinformation or disinformation online – how should I respond?

Fake News, misinformation and disinformation have never been more widespread. This is a serious problem for everyone, and can have significant impact on the wellbeing of children and young people. Research by the Commission on Fake News and Critical Literacy in Schools reported that fake news can have a harmful effect on children's wellbeing by increasing levels of anxiety, damaging self-esteem, and skewing their world view.

The links below have a range of useful resources that can help adults talk to children and young people about specific concerns or incidents as well as how to develop and embed a systematic approach to digital literacy, which will better protect everyone from the harm that fake news can cause.

Tips on how to talk to children and young people about fake news (for families and practitioners):

- Internet Matters
- NSPCC
- BBC Bitesize
- The Literacy Trust

Systematic approaches and curriculum resources (for practitioners):

- Educate Against Hate
- Newswise
- The Citizenship Foundation (Conspiracy Theories in the Classroom)
- Be Internet Citizens
- Shout Out UK

I have heard about a harmful or distressing challenge/content circulating online. I'm not sure if it's true or not but how should I respond?

The internet and social media provide a perfect platform for viral videos, challenges, and hoaxes, especially trends that are said to be harmful, to be spread quickly. A hoax is a deliberate lie designed to seem truthful, and online challenges generally involve users recording themselves taking a challenge, and then distributing the video through social media channels, inspiring or daring other to repeat the challenge.

If you are made aware of a viral concern circulating online, you should speak with your agency designated safeguarding lead who will be best placed to lead and provide any formal responses, if deemed necessary. They should undertake a case-by-case assessment, establishing the scale and nature of the concern. Quick local action may prevent a local online hoax or harmful online challenge going viral (quickly and widely spread).

As professional organisations with a duty to safeguard our clients, we need to ensure that we are only sharing factual and useful information. Your designated safeguarding lead should check the factual basis of any harmful online challenge or online hoax with a known, reliable and trustworthy source, such as KSCMP/MSCP or the Professional Online Safety Helpline from the UK Safer Internet Centre. Education settings can seek specific advice from the Education Safeguarding Service.

Naming an online challenge or hoax and providing direct warnings about specific apps or games is usually counterproductive. Concerns are often fuelled by unhelpful publicity and may not be based on confirmed or factual occurrences or any real risks. There have been examples of hoaxes where much of the harmful content was created by those responding to the story being reported, which increased vulnerable users' exposure to distressing content. Even with real challenges or concerns, many clients may not have seen the content or be aware of it. Organisations must carefully weigh up the benefits of highlighting the potential harms related to a challenge, against needlessly increasing exposure to it. Professionals should always avoid sharing upsetting or scary content; exposing clients to upsetting or scary content will be counterproductive and potentially harmful.

If you are confident your clients are aware of, and/or are engaged in a real challenge that may be putting them at risk of harm, then it would be appropriate for this to be directly addressed with them and their families. Carefully consider how best to do this; it may be appropriate to offer focussed support for individuals at risk.

Whilst aimed at education settings, professionals may find the following links helpful when considering how best to respond to viral concerns:

- DfE: Harmful online challenges and online hoaxes
- The Education People: 'Think before you scare'
- UK Safer Internet Centre: De-escalating and responding to harmful online challenges

How can I recognise if the time someone is spending online is harmful to them?

The online world is a central part of daily life, and it is important to be able to recognise what is essential or usual online use and what could be considered harmful. Harm is something that is experienced uniquely by each person. What could be harmful for someone, might not be harmful for someone else. However, there are some general indicators to help identify when something is harmful. For example, has the young person's relationships suffered as a result of their online use? Are they not seeing friends, or going out as much? Do they seem moody, upset or withdrawn? Do you feel as though they are being secretive about what they are doing online? Are they making statements that do not fit with British Values? If any of these things are a worry, further advice should be sought.

Professionals may find the following links helpful when exploring screen time and promoting balanced use of technology:

- Royal College of Paediatrics and Child Health: The health impacts of screen time – a guide for clinicians and parents
- Internet Matters: Screen time advice

- Childnet: Screen time and healthy balance
- GamCare
- Big Deal?
- The National Centre for Gaming Disorders

I think someone is at risk of cybercrime – how can I support them?

Cybercrime is criminal activity committed using computers and/or the internet. It is broadly categorised as either 'cyber-enabled' (crimes that can happen off-line but are enabled at scale and at speed on-line) or 'cyber dependent' (crimes that can be committed only by using a computer).

Cyber-dependent crimes include:

- unauthorised access to computers (illegal 'hacking'), for example accessing a school's computer network to look for test paper answers or change grades awarded, or a workplace network to delete files
- 'Denial of Service' (Dos or DDoS) attacks or 'booting'. These are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources, and,
- making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including those above.

If you are concerned someone you are working with is at risk of cybercrime there are a variety of ways you can support them to reduce the chances of them becoming a victim, as well as organisations and resources you can signpost to for further support.

As soon as an incident occurs it should be reported to the Action Fraud team by calling 0300 123 2040, and they will provide the help, support and advice needed. If someone is being subjected to a live and ongoing cyber-attack, contact Kent Police on 101.

Children and young people with particular skills and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime. If there are concerns about a child in this area, professionals should consider referring into the Cyber Choices programme. This is a nationwide police programme supported by the Home Office and led by the National Crime Agency, working with regional and local policing which aims to intervene where young people are at risk of committing, or being drawn into, low-level cyber-dependent offences and divert them to a more positive use of their skills and interests.

Professionals may find the following links helpful when considering how best to respond to concerns and/or provide advice on how to stay safe online:

- Kent Police – Cybercrime/Fraud
- The National Cyber Security Centre (NCSC)

- Action Fraud
- National Cyber Resilience Centre Group
- NCA - Cyber Choices

Someone has told me that they are being bullied or harassed online. What advice can I give them?

The responsibility for dealing with online bullying is shared. It will require co-operation between those involved, their families, professionals and schools or other education settings to ensure that situations are identified and managed appropriately.

Online or cyberbullying is the use of technology 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 and may be unaware of the laws regarding harassment and the fact online activity can be traced. Electronic content is 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, for example '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 you believe that a crime has been committed, then seek assistance from the police via 101. If it is an emergency, for example someone is injured, in danger or there is an immediate risk to someone's life, you should contact 999.

If someone discloses online 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 they report content to a website and it is not removed, in some circumstances, concerns can be reported to the Report Harmful Content website for additional reviews.

If they are being bullied by known individuals such as peers at school, the education setting should be involved to support and sanction learners according to their anti-bullying and behaviour policies. Section 89 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, and if bullying outside of school involving learners is reported, then it should be investigated and acted on. Education settings can seek specific advice from the Education Safeguarding Service.

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

It is essential for professionals to recognise the importance of disclosing an online safety concern, especially for children and young people. Often children and young people are fearful of talking about online dangers with adults as they believe the adult will dismiss the issues, for example '*I don't understand technology, I wish it could be banned'* or are fearful of being punished or blamed and having their devices or internet access taken away. It is essential 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 can lie about or hide their behaviour which leads to them being more vulnerable online.

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

You should always follow your organisations policies and procedures if someone shares an online concern with you. You should ensure you do not promise confidentiality and 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, for example '*tell me…, explain what…, describe how…'.*

Professionals should not ask questions to gather opinions, such as '*why did you do that?'* as this can make young people feel like that they are to blame. Victim blaming is any language or action that implies (whether intentionally or unintentionally) that a person is partially or wholly responsible for abuse that has happened to them. It is harmful and can wrongfully place responsibility, shame, or blame onto a victim, making them feel that they are complicit or responsible for the harm they have experienced. Children can never be expected to predict, pre-empt, or protect themselves from abuse, and irrespective of the content or circumstance, the responsibility always lies with the person who abused the child or young person. It may be helpful for professionals to access the UK Council for Internet Safety's 'Challenging victim blaming language and behaviours when dealing with the online experiences of children and young people' guidance as it offers practical steps to help professionals practice and advocate for an anti-victim blaming approach, in a constructive and supportive way.

Staff should never request that the 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 an online concern should be the designated safeguarding lead within your organisation – professionals should not attempt to handle online abuse situations alone. You should record your concerns as soon as possible using the child or young person's own words.

They should be reassured and supported at all stages and involved as far as possible (according to their age and ability), for example speaking to the safeguarding leads, reporting concerns directly to the platform or external reporting mechanisms.

Social workers working with children and young people who make disclosures regarding online abuse should follow child protection Section 47 enquiry procedure. 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 – what support is available for them?

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

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

- The NCA CEOP Command (formerly the Child Exploitation and Online Protection Centre) delivers a multi-agency service dedicated to tackling the abuse and exploitation of children. A key focus of CEOP is the Think U Know website and education strategy to teach young people, professionals and parents/carers about online safety and has a report abuse button to report online sexual abuse or suspicious behaviour. Any reports of abuse made are 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.

Stop it Now! www.stopitnow.org.uk

- Stop it Now! UK and Ireland is a child sexual abuse prevention campaign run by the Lucy Faithful 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 of 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

Report Harmful Content: https://reportharmfulcontent.com

- Report Harmful Content can help people report harmful content online by providing up to date information on community standards and direct links to the correct reporting facilities across multiple platforms. Report Harmful Content supports reporting on eight harms: threat, impersonation, bullying or harassment, self-harm or suicide content, online abuse, violent content, unwanted sexual advances and pornographic content.

Revenge Porn Helpline: https://revengepornhelpline.org.uk

The Revenge Porn Helpline is a UK service supporting adults (aged 18+) who are experiencing intimate image abuse, also known as revenge porn. The Helpline was established in 2015 alongside the legislation which made it an offence to share intimate images or videos of someone, either on or offline, without their consent with the intention of causing distress.

How can I find out more about online safety?

Professionals should be encouraged to access appropriate online safety training and guidance 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 designated safeguarding lead for further information.

KSCMP/MSCP also provides multi-agency training for professionals and advice on their websites. Education settings can seek specific advice from the Education Safeguarding Service.

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

If you believe there is evidence of misconduct by any members of your organisation, then this should be reported to your designated safeguarding lead and/or follow your organisations whistle blowing policy and procedures.

Headteachers and managers should seek advice via the Local Authority Designated Officer (LADO) if there is an allegation being made against a member of the children's workforce. KSCMP/MSCP provide advice on the process to follow on their website. Additional support may be accessed via HR/Personnel Services, Social Services, or the Police, if appropriate.

3. Frequently Asked Questions: Keeping Myself Safe Online

Please be aware that staff should always follow their organisations appropriate policies; for example, codes of conduct, acceptable use policies (AUP), safeguarding reporting mechanisms and professionals' standards, for example, Teaching Standards and Social Work England.

Can my organisation limit my 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 children's workforce (including for example, teachers, social workers, early years staff), 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 service user or their family members 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 or messages were copied and shared by anyone with access, 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 we work with in a shop queue might be overheard, 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.

You should ensure you are fully conversant with the security and privacy setting for any sites you use and should always avoid posting any information or content which could compromise your professional integrity and any associated professional standards or organisation expectations.

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 or your profile has been set correctly and a strong password used, information should remain relatively private. Social networking is a way of life for many children and young people, however professionals working with vulnerable groups should carefully consider their use of social networks as they take on professional responsibilities. Strong passwords should be used, and appropriate security or privacy settings should be applied so that you can control all access to your profile and content.

However, it's important to be aware that once published, information such as photographs, comments, blog posts or other online content are almost impossible to control and can potentially be shared and manipulated without your consent or knowledge. Some users 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, commenting on a public news story, or liking a post which contains offensive language, could be misinterpreted.

Fictitious 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 and generally use automated registration systems which 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, these records can be edited. It is essential that staff protect their professional reputation, both on and offline and follow their individual agency policies and procedures.

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 you do not maintain your online identity, 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 identify any publicly available content, such as social media posts, websites, or images. If you see anything which is concerning, 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. 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 yourself or 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. Be mindful of commenting on friend's content or on any public news stories 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 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.

Think carefully about who you are friends with online, and which friends can access what information. It is a good idea to considering remove any ‘friends’ who could compromise your professional role, however if there is a pre-existing relationship, 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 and/or your line manager.

It is strongly recommended that professionals do not list their place of work on any of 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. Sadly, there have also been cases where staff working with vulnerable groups have been targeted by online criminals or sex offenders; as such it is recommended that professionals consider keeping this information private on all online communication tools, such as dating apps or websites.

If you are approached or contacted by a child, young person, or family member of a service user 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 LinkedIn or Twitter to take part in professional development events such as joining in discussions at a conference or event, then you should consider creating a separate and distinct social media presence. This will ensure that professional boundaries are maintained, and you are able to safeguard your personal and professional image 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 or email address, but they can put in place expectations regarding safe online behaviour and use of technology and devices within the workplace. This is especially important if you work directly with children, young people, and families.

If it is provided, it is a good idea to lock your personal devices in a safe and secure place unless you are using them, for example lock your mobile phone in a drawer or locker until your lunch break.

It is recommended that you ensure your personal devices are suitably protected for example, by using biometric IDs, PIN, password, or passcode to prevent accidental or deliberate misuse. Some professionals have had their reputation undermined or have placed themselves or others at risk following clients accessing personal photos and details stored on devices. Examples could include service users accessing your personal details, such as where you live or accessing your personal photos or using your device to access illegal or inappropriate content.

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 for example 1234, 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 help to prevent identity theft. Useful advice on setting safe and strong passwords can be found here.

You should be aware that for some devices, information and apps may still be accessed even if a phone is locked and it is important to ensure that appropriate settings are applied to devices 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 system following use as this will prevent people posting content or accessing private information.

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

Children, young people and adults are encouraged to report concerns, and this may involve the use of new technology. Many young people 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 professionals and their clients may not be inappropriate, but it might look very different if carried out via email or social media, and this can lead to difficulties and possible allegations if misinterpreted, forwarded or used out of context. Care in the use of appropriate electronic signatures or any usernames selected is required when communicating within a professional setting. You should be aware of, and comply with, your organisations policy on the use of text or social media and be circumspect in your communications with clients to avoid any possible misinterpretation of your motives or any behaviour which could be construed as grooming or abusive.

Should I have children, young people and/or adults I support as 'friends' or contacts on my personal social media account 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/young people or adults, and when appropriately arranged, can guide, and enhance such activities.

Communication, by whatever method, should always take place within clear and explicit professional boundaries. Professionals should not share any personal information with children, young people or adults they support. Staff should not request, or respond to, any personal information from children, young people or adults they support, other than that which might be appropriate as part of your professional role and in accordance with your agencies code of conduct. You should ensure that all communications are transparent and open to scrutiny. Consideration should always be given as to how communication via informal and/or personal communication channels might appear to a third party. Compared with a conversation within a formal workplace environment, for example your official work email address, the use of social media increases the potential for messages to be taken out of context or misinterpreted.

Professionals should use an online environment which is under their control. An officially provided communication and collaboration area will have a range of security features set within a policy framework. Logs should be available in case a concern or allegation is raised.

It is strongly recommended that professionals do not add children, young people or family members you only know through your professional role as 'friends' or contacts on any personal social media services. By adding or accepting such requests you will be sharing personal information about yourself or will have access to personal information about the children, young people or families you are supporting. You could potentially leave yourself vulnerable to allegation of inappropriate contact or conduct or find yourself exposed to unwanted contact. Your organisation should provide guidance regarding this in their behaviour policy, code of conduct, or acceptable use policy (AUP).

Personal email addresses, instant messaging identifiers, social networking accounts or telephones (fixed or mobile) should never be used to contact any children, young people or families you are supporting. Work provided/managed emails and phone numbers should be used if communication with clients is required. If sudden or urgent communication is required, this should be discussed and approved by your designated safeguarding lead or line manager. If social media use is required, then a separate professional account or contact should be used, with the agreement of management, following an appropriate risk assessment. Any decision should be formally recorded.

Any pre-existing relationships or exceptions which may compromise this, for example your own children are pupils at the school you work at, or a parent is a family member or long-time friend, should be discussed with your organisations designated safeguarding lead and/or line manager. This will help to ensure that the relationship is formally acknowledged and will enable your designated safeguarding lead/line manager to discuss with you your organisations expectations regarding professional conduct.

Should I use my personal mobile phone or device to take photographs or videos of clients?

It is important to continue to celebrate achievements of children, young people and adults we support through the appropriate use of photography, however there are potential dangers.

The safest approach is to avoid the use of any personal equipment and to use an organisation or agency provided device. One potential danger is an allegation that a member of staff has taken an inappropriate photograph; with a personal camera it would be more difficult for staff to prove that this was not the case but if using organisation equipment there is a demonstration that the photography was consistent with the organisations policy.

Staff should always ensure they have appropriate consent to take photographs and videos to ensure compliance with Data Protection legislation. Organisations must have written parental consent to take, store and use images of children, and where the subject of the photograph is 13+, they may be able to provide consent themselves.

Care must be taken to ensure photographs are stored appropriately and in accordance with the law. For instance, copying photographs onto 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 CDs 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 used, 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 manager and/or designated safeguarding lead and you must always follow data protection legislation and ensure that children, adults and staff are appropriately safeguarded. Any images taken should not be shared or posted on 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 designated safeguarding lead and data protection officer/lead within your organisation.

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. Clients and their families 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, including 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 platform where the comment/content was posted terms and conditions, then content posted online cannot always be forcibly removed. The best course of action is to adopt a partnership approach and for designated safeguarding leads 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 client, their family member or colleague, for example a parent makes inappropriate comments about you, don't retaliate, and make sure that you save any evidence such as posts, URLS, messages, comments, names, times, dates and locations. You should report your concerns to your designated safeguarding lead and/or line 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 Professional Online Safety 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.

I'm concerned about the online behaviour of a colleague – what should I do?

It is crucial that any concerns staff have about their colleagues are shared and reported responsibly to the right person and are recorded and dealt with appropriately.

Organisations should have clear policies which explain what behaviour, both on and offline, is and is not acceptable – this is usually found within a code of conduct or staff behaviour policy and may also be in line with any associated professional standards and expectations, for example Social Work England registration or Teaching Standards. Organisations will have policies to follow where there are concerns about staff members conduct and this should include if there are concerns about staff online behaviour or activity.

KSCMP/MSCP guidance should be followed in any cases where it is alleged that a person who works with children, in either a paid or unpaid (volunteer) capacity, has:

- Behaved in a way that has harmed a child, or may have harmed a child
- Possibly committed a criminal offence against or related to a child
- Behaved towards a child or children in a way that indicates they may pose a risk of harm to children
- Behaved in a way that indicates they may not be suitable to work with children (includes transfer of risk, risk by association).

Working Together to Safeguard Children 2018

Allegations against people who work with children or young people should be reported immediately to a senior manager within the organisation, for example in schools this is usually the headteacher or chair of governors. The senior manager should inform the Local Authority Designated Officer (LADO) within one working day. The LADO's role is to oversee allegation management in providing proportionate advice and guidance to help senior leaders undertake the most appropriate course of action and to ensure the safety of children and the member of staff.

There may however be other concerns noticed where a member of staff's online behaviour does not meet the threshold for an allegation, however, is inconsistent with the staff code of conduct; this could include inappropriate conduct online or behaving inappropriately when using technology as part of their role. It is important that any concerns are shared with senior managers as this will enable organisations to identify concerning, problematic or inappropriate online behaviour early, minimise the risk of abuse, and ensure all staff are acting within appropriate online professional boundaries, in accordance with the ethos and values of the organisation. In these cases, action should be taken in line with any organisation policies and appropriate disciplinary action should be taken following any advice from personnel or Human Resources (as appropriate).

I've seen something harmful or hateful online – what should I do?

Harmful content is anything online which causes a person distress or harm. This encompasses a huge amount of content and can be very subjective depending on the viewer; what may be harmful to one person might not be considered an issue by someone else.

If you see posts or content online that worry you, you should report it, even if you're not sure of the community guidelines on a site or platform. You can usually find community guidelines by going to settings in an app, or policies on a website.

Report it on the site: sites and platforms have different processes, and you should be able to find information about how to make a report on the site or app. Reporting content to the site or platform where it is hosted means it can be reviewed by their moderators and removed if it breaks community guidelines, which means that fewer people will be upset by seeing it.

Visit the Report Harmful Content website: if you are unsure of how to make a report about self-harm or suicide content or have seen the same content in lots of places online, then use the Report Harmful Content website, which has step-by-step information on how to make a report on some of the most popular social network and video sharing platforms. They can also help if you have already reported harmful content to a site and there has been no resolution. The Report Harmful Content website is run by the UK Safer Internet Centre.

4. Frequently Asked Questions: Keeping Data and Systems Safe

Please be aware that staff should always follow their organisations appropriate policies, for example codes of conduct, acceptable use policies (AUPs) and safeguarding report mechanisms.

How should I store personal data safely?

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

The Data Protection Act (DPA) 2018 and UK General Data Protection Regulations (UK GDPR) 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 always be kept secure. 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 your children or other family members may have access to) and laptop theft from a vehicle are all too common. You 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 will be using your work network, which should have a remote backup facility.

Information security is an integral part of the Data Protection Act and UK GDPR. 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 Kent and Medway Council guidance available.

You must take care to prevent others gaining access to information accessible via your work account, particularly when using work mobile phones and laptops in areas where clients 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. You should always lock your device or use pin/passwords to protect them when they are not in use and should always log out of systems and accounts when you have finished using them.

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

Could 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 and therefore in accordance with the Data Protection Act 2018 and UK GDPR.

Any files (paper or electronic), containing personal data must always be stored in accordance with the Data Protection Act and UK GDPR; 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, and Freedom of Information, and your organisation must ensure it is compliant with legislation and can meet its statutory safeguarding responsibilities.

You should be aware that cloud computing may not be appropriate for all users, especially where security of confidential data and personal data is involved. Cloud storage should not be used unless it fully meets data protection requirements and is suitably protected/encrypted. It is not advisable to use cloud storage to store any content or files which would be considered confidential, or which may be subject to the DPA, for example information that contains personal information or where content may be hosted outside of the EU.

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 line manager, DSL, and/or information governance/data protection lead/officer.

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

Personal use of technology 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 your professional use only.

Things that can go wrong include:

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

Professionals should refer to the organisations policy on the personal use of work devices, which may vary between organisations. Increasingly the use of a work device for non-professional use is being explicitly banned. Professionals should always ensure that they have absolute control of 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 organisations network use?

Filtering or monitoring network usage will only be effective if it is regularly and carefully reviewed to notice and report inappropriate access or usage. Often this places a responsibility on technical staff which they may not have been trained for. This responsibility can become onerous if a client or staff member is implicated in inappropriate or illegal activity.

It is wrong to assume that filtering and monitoring are simply technical IT activities, solely managed by the network staff. Some technical staff may have indeed taken on this wider responsibility to help ensure that IT 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 should work together with designated safeguarding leads 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 safeguarding 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 designated safeguarding lead. Procedures to preserve evidence by unplugging a computer or locking an account need to be in place.

The filtering and monitoring policy for organisations should be agreed by the designated safeguarding lead and managers, with set procedures to deal with incidents. Senior managers should ensure that member of technical staff are supported in their role in maintaining the ability to monitor the network when making purchasing decisions. For example if a member of staff buys a set of tablets to use with young people, the technical staff should be involved to ensure that devices are compatible with current systems or can be managed in accordance with the organisations legal safeguarding requirements as outlined within the Prevent Duty, and for school and colleges, Keeping Children Safe in Education.

A common concern found in these situations is that non-technical staff may not be aware that without an identifiable user (for example, 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 organisations network and it was discovered that a user was accessing indecent images of children or extremist content, it would be difficult and, in some cases, impossible to work out who was responsible and could mean that organisations are not complying with their statutory safeguarding responsibilities and could ultimately place our communities at risk of significant harm.

Further advice regarding appropriate monitoring and filtering in education settings can be found via the UK Safer Internet Centre. The advice may also be helpful for other organisations.

5. Useful Links and Resources

Kent and Medway links

- Kent information governance for education settings: www.kelsi.org.uk/school-management/data-and-reporting (KCC staff should also access Knet for further information)
- Kent Safeguarding Children Multi-Agency Partnership: www.kscmp.org.uk
- Medway Safeguarding Children Partnership: www.medwayscp.org.uk/mscb
- Kent Police: www.kent.police.uk/internetsafety

National links for reporting concerns

- NCA-CEOP: www.ceop.police.uk/ceop-reporting
- IWF: www.iwf.org.uk
- Report Harmful Content: https://reportharmfulcontent.com
- Report Terrorist Content: https://act.campaign.gov.uk
- Stop It Now Helpline: www.stopitnow.org.uk

National online safety advice, guidance, and resources

- Childnet: www.childnet.com
- Internet Matters: www.internetmatters.org
    - Internet Matters – Inclusive Digital Safety: www.internetmatters.org/inclusive-digital-safety
- NCA-CEOP Think U Know: www.thinkuknow.co.uk
- NSPCC: www.nspcc.org.uk/onlinesafety
    - NSPCC online safety for families and children with SEND: www.nspcc.org.uk/keeping-children-safe/online-safety/online-safety-families-children-with-send
- Parents Protect: www.parentsprotect.co.uk/
- Parent Zone: https://parentzone.org.uk/
- UK Council for Internet Safety (UKCIS): www.gov.uk/government/organisations/uk-council-for-internet-safety
- UK Safer Internet Centre: www.saferinternet.org.uk

National guidance for organisations and managers

- Safer Recruitment Consortium: https://saferrecruitmentconsortium.org
- National Education Network: www.nen.gov.uk
- Professional Online Safety Helpline: https://saferinternet.org.uk/professionals-online-safety-helpline