Online Safety

thirtyone:eight

Creating safer places. Together.

Welcome to the Thirtyone:eight Online Safety course. This handbook is designed to accompany the webinar and contains the case scenarios, discussion questions and polls we will be using in the webinar.

Online Safety is a four UK nations friendly course. Most of the information in the handbook is applicable to all four nations, but where legislation varies between nations this will be highlighted. This handbook has a lot of information and isn't designed to be read cover-to-cover. We encourage you to use the contents page to identify the information relevant to you, and to revisit this information when you need a refresher and as things arise.

As we begin, it is good to define what we mean by online safety. Here is Thirtyone:eight's definition:

Online safety is the collective term for safeguarding involving the use of electronic devices and applications to communicate and access the Internet; often referred to as Information and Communications Technology.

This course will enable you to recognise your organisation's responsibilities to keep people safe online. It will equip you to create policies and practices to outwork this in practical ways. The online world is changing rapidly so we will not focus on specific platforms, rather the overarching principles related to different aspects of online safety.

We will consider the four areas of: content, contact, conduct and commerce[1]; raising awareness of potential risks and thinking through how to reduce them. This handbook will also signpost you to other resources that will keep you up to date with the newest developments in the online space.

We are looking forward to supporting you as you safeguard those you work with through your Online Safety processes.

The Thirtyone:eight team

[1] The original source of the 4 'C's of online safety is: Livingstone, S., & Stoilova, M. (2021). The 4Cs: Classifying Online Risk to Children: https://doi.org/10.21241/ssoar.71817 .It has since been adopted into guidance such as Keeping Children Safe in Education (KCSIE) and the 2023 Department for Education safeguarding guidance for after-school clubs, community activities and tuition.

Contents

Questions and Exercises in the Webinar

Throughout the webinar there will be opportunities to have discussions, share knowledge and participate in activities to apply our learning in context. These are included here for reference only. There is no need to work through anything in advance.

Introduction:

Pause and consider: What would be a good outcome for you today? *Think about- What's brought you here? What is your role? What are you hoping to gain?*

Module 1: Content

Pause and consider: What harmful content are you aware of?

Breakout rooms: How can we reduce the risks posed by harmful content?

Module 2: Contact

Pause and consider: Think about your context. Who do you contact in your role? What other online connections are there in your community?

Consider the following case scenario: Rachael is 37 and is a volunteer youth leader for your organisation. Her own children are in the pre-school group and she and her family have been members of your community for a number of years. She's a popular leader and lots of the young people look up to her and ask her for advice about friendships, school etc. She's accepted a couple of social media requests from young people in the group and recently one of the girls started to message her privately after getting her number from the youth WhatsApp group. They have been messaging daily, often in the evening, about difficult relationships the girl has been having at school. The girl's parents have raised a concern because they have found out about this.

1. **What are the risks in this situation?**
2. **What are your safeguarding responsibilities?**

Module 3: Conduct

Pause and consider: What types of harmful online conduct are you aware of?

Consider the following case scenario: It's the first evening of your summer camp, one of the young people comes to talk to you. Harper is 13 years old and is quite shy and quiet. When you ask how they're doing Harper starts crying and explains, "The night before camp I was at a party. I've got some older friends - they gave me alcohol. It's the first time I tried it. I thought it was fun but now there's videos of me doing really, really embarrassing things all over social media. It's so shameful. At school they told us, 'Once it's online it's there forever' so that's it for me now. There're already loads of comments. All my friends will see, my family – I'll be in so much trouble. I just can't face it."

1. **What are your concerns?**
2. **What are your safeguarding responsibilities?**

Module 4: Commerce

Consider the following case scenario: Donal is 83 and attends your seniors' lunch every Wednesday. Today he arrives late and looks flustered. When you ask if he's ok, he says: "I will be once I get this bank business sorted. They sent an email in the middle of the night - someone has used my card! I just need to type in my details so they can fix it. Trouble is, I can't remember them. I wrote the password and things in my diary but that's not in the usual drawer. I've turned the place upside down! My daughter will be over later so she can help me look. I've just come out to clear my head."

1. **What are your concerns?**
2. **What are your safeguarding responsibilities?**

Pause and consider: What other online financial risks are you aware of?

Online Safety Mini Audit Tool

The following tool is designed to help you identify what online safety measures you already have in your organisation and what your next steps might be to make your organisation even safer. For each statement, decide if this is something you already have in place, something you don't have yet but need, or something that is not relevant to the work of your organisation. You can also use this tool to review your Online Safety Policy.

Online Safety Consideration:	Have	Need	N/A	Review Date
General				
We have an online safety policy.				
The online safety policy has been reviewed recently.[2]				
We have nominated someone to oversee online safety.				
Content				
Our policy tells people what to do if they see / experience harmful content.				
Our policy tells people what content cannot be accessed on our organisation's devices.				
We have acceptable usage agreements for staff and volunteers.				
Staff and volunteers know what will happen if they violate acceptable usage agreements.				
We use filters to block inappropriate content on our organisation's devices and WiFi settings.				
Staff and volunteers use strong passwords to protect our organisation's devices.				
We regularly update wifi passwords.				

[2] Your organisation's main safeguarding policy should be reviewed annually. Other related policies should be reviewed on a regular, scheduled cycle agreed by trustees and as and when significant changes occur between scheduled reviews (e.g. changes to those in responsible roles, changes to the way you work, changes in law etc).

Staff and volunteers use individual log in details to access our organisation's devices.				
We have guidelines about what content can be displayed on our website and social media.				
Only authorised individuals can update the website and social media pages.				
We seek permission before any images are taken or displayed and images are only used for the specific purpose for which permission was sought.				
Live streaming is clearly advertised in advance of and during events, and we seek parental permission where children are involved.				
Children's full names are not displayed on the website or social media pages.				
Contact				
Our policy tells people what to do if they are worried about any online contact.				
Our policy and / or codes of conduct give clear guidelines for contacting vulnerable groups[3] online (including via messaging services).				
Our staff and volunteers use organisational email addresses for any contact related to their role.				
We risk assess any online activities that involve contact with and between vulnerable groups.				
Vulnerable groups know what to expect from our staff and volunteers in terms of online contact.				
Staff and volunteers are supported and supervised to be transparent and accountable in their online contact.				

[3] Children, young people and adults at risk of harm.

Those who manage our social media accounts, update our website and send communications on behalf of our organisation have clear codes of conduct around safe online contact.				
We have clear policies and procedures about safe storage, use and sharing of personal data including contact numbers and email addresses.				
Conduct				
Our policy tells people what to do if they see or experience harmful online conduct.				
Codes of conduct for all roles in our organisation include online conduct as necessary.				
Staff and volunteer training and induction include expectations of online conduct.				
Staff and volunteers in our organisation model safe behaviours in our personal online conduct.				
Staff and volunteers are trained to respond to concerns from vulnerable groups in ways that provide reassurance and reduce shame.				
We have clear reporting procedures for harmful online conduct – always report internally; external reporting as appropriate – statutory services, Barring Service / PVG, Charity Regulators as necessary.				
Commerce				
Our policy tells people what to do if they or someone else may have been targeted by online extortion, fraud, blackmail or other financial harms.				
We have clear policies and procedures around data retention, storage and sharing.				

We ensure we have strong privacy settings on all our organisation's accounts.				
We offer training, support and accountability for safe online transactions for all budget holders.				
We use multifactor authentication (MFA) on our organisation's devices.				
We have clear guidelines for staff and volunteers about regularly updating and safely storing passwords.				
We have nominated someone to oversee our IT systems to ensure they are safe and secure.				
Related Policies				
Our anti-bullying and harassment policy acknowledges these behaviours can also take place online.				
We have a Data Storage and Handling policy that takes into account digital data and GDPR requirements.				

Relevant laws across the 4 UK nations

Safeguarding practice is usually based on the laws made by one of the 4 UK Governments (Westminster, Stormont, Holyrood and the Senedd). You do not need to memorise or have a deep understanding of these pieces of legislation, it's enough to have an awareness that there is a legal framework that informs how we keep people safe online.

For those interested in the details, the key pieces of legislation related to Online Safety for each UK nation are listed below. The full legislation documents are available online by searching the name and date given here. Appendix 2 gives further information on the Online Safety Act 2023, which applies to all 4 nations of the UK.

UK Wide Legislation
Online Safety Act 2023 Data Protection Act 2018 Criminal Justice and Courts Act 2015 Communications Act 2003 Sexual Offences Act 2003

England	**Northern Ireland**	**Scotland**	**Wales**
Safeguarding Vulnerable Groups Act 2006	Safeguarding Vulnerable Groups (Northern Ireland) Order 2007	Protection of Vulnerable Groups (Scotland) Act 2007 Police Act 1997 (as amended)	Safeguarding Vulnerable Groups Act 2006
'Position of trust' offences within ss.16 – 19 of the Sexual Offences Act 2003 now include situations where certain activities take place in a sport or religion (as	Section 5 of the Justice (Sexual Offences and Trafficking Victims) Act (Northern Ireland) 2022 known as 'Abuse of Position of Trust'	'Positions of trust' law in Scotland remains as originally set out in the Sexual Offences Act (2009), which does not cover religious or sports settings.	'Position of trust' offences within ss.16 – 19 of the Sexual Offences Act 2003 now include situations where certain activities take place in a sport or religion (as amended by the Police, Crime,

amended by the Police, Crime, Sentencing & Courts Act, 2022).			Sentencing & Courts Act, 2022).
Malicious Communications Act 1988	Malicious Communications (Northern Ireland) Order 1988	Defamation and Malicious Publication (Scotland) Act 2021	Malicious Communications Act 1988
Stalking Protection Act 2019	Protection from Stalking Act (Northern Ireland) 2022	Criminal Justice and Licensing (Scotland) Act 2010	Stalking Protection Act 2019
The Protection of Children Act 1978 (as amended by the Criminal Justice and Public Order Act 1994). This law criminalises the taking, distribution and possession of an "indecent photograph or pseudo-photograph of a child".	The Protection of Children Act 1978 (as amended by the Criminal Justice and Public Order Act 1994). This law criminalises the taking, distribution and possession of an "indecent photograph or pseudo-photograph of a child".	The Protection of Children Act 1978 (as amended by the Criminal Justice and Public Order Act 1994). This law criminalises the taking, distribution and possession of an "indecent photograph or pseudo-photograph of a child". Also Sections 52 and 52A of the Civic Government Scotland Order.	The Protection of Children Act 1978 (as amended by the Criminal Justice and Public Order Act 1994). This law criminalises the taking, distribution and possession of an "indecent photograph or pseudo-photograph of a child".

Appendix 1: A-Z of Online Safety Terms

You may come across the following terms when reading about online safety. There are many more we could have included here. There are links to other resources explaining terminology in the signposting section of this handbook:

Anti-Virus: A program that prevents, detects and removes malware or viruses.

App (Application): A program with a specific purpose that can be installed on to a mobile device.

Artificial Intelligence (AI): Computer systems able to perform tasks usually requiring human intelligence.

Attachment: Files, such as photos or documents, sent with an email or social media post.

Block: To prevent someone contacting you or viewing your social media profile.

Bluetooth: A method of exchanging data over short distances.

CAIC: Acronym for 'child abuse images and content'.

Catfishing: Creating a fake online persona with the intent to deceive, often linked to romance fraud or financial scams.

CEOP: Acronym for Child Exploitation and Online Protection command. An organisation within the National Crime Agency to protect children and young people from online abuse and grooming.

Clickbait: Online content designed to attract attention, so users click a link. Clicking the link generates income for the site.

Content filter: A way of restricting access to inappropriate online content.

Creeping: Following someone's social media activity to an excessive degree.

Cyberbullying: Bullying behaviour that takes place online.

Cyberstalking: Following or harassing someone using technology. A pattern of behaviour that causes emotional harm.

Dark Web: An area of the internet associated with illegal content and criminal activity.

Decoy App: Also known as ‘secret’ or ‘ghost’ apps. On the surface it has one purpose, but actually stores photos, videos or messages the user doesn’t want others to see.

Deepfake: Using Artificial Intelligence and technology to seamlessly superimpose a person's image into videos or photographs that they never actually participated in.

Doxxing: Searching the internet for private information on a person or organisation with the intent to publish it and cause harm.

E-commerce: Online shopping.

Encryption: Turning messages into code to hide the information’s true meaning so it can’t be read by someone intercepting it.

Fake News: Term to describe untrue, unreliable or misleading information.

Firewall: A virtual barrier to prevent hackers or malware gaining access to an individual or organisation’s computer system via the internet.

Flaming: Sending provocative messages likely to cause offence or start and argument.

Gamertag: An alias used to represent a player in online games.

Griefer: A player who deliberately harasses or upsets other players in online games.

Grooming: When a perpetrator develops a relationship with a child, young person or at-risk adult in order to harm them.

Hacker: Someone who attempts to gain unauthorised access to computer systems.

Identity Theft: Impersonating someone else by using their personal details, often for financial gain.

IAP: Acronym for in-app purchases – features a user can buy within a ‘free’ app or game.

Influencer: An online celebrity who can influence perceptions via social media due to a large number of ‘followers’.

Junk Mail: Unwanted or unsolicited emails, usually marketing or advertising.

Livestream: Sharing video content in real time.

Malware: Short for 'malicious software'. Collective term for programs designed to cause harm to computer systems.

Parental controls: Tools to monitor and protect children's access to the internet.

PEGI: Acronym for Pan European Game Information – age classification system for games in the UK.

Persuasive design: Features in apps designed to reward increased usage or penalise decreased usage.

Pharming: Scam used to gain personal information. Users are unknowingly redirected from a genuine site to a duplicate site which is used to extract confidential information.

Phishing: Scam often carried out via email where users are misled into revealing confidential information such as bank details or passwords.

Profile: Information about a person visible on social media platforms.

Quishing: QR Code phishing – often used on car parks (*See phishing)

Radicalisation: Inciting someone to hate or harm.

Ransomware: A type of malware that renders a computer system unusable until money is paid.

Revenge Porn: The illegal posting or sharing of adult sexual photos or videos without a person's consent in order to cause harm.

Selfie: Photo you take of yourself.

Sexting: Sending or receiving sexually explicit photos, messages or videos.

Sextortion: Being forced to pay money after an offender has threatened to release nude or semi-nude pictures of the victim.

SGII: Acronym for Self-Generated Indecent Images. Indecent sexualised images that an individual takes of themselves, voluntarily or under coercion.

Sharenting: Term referring to parents sharing pictures and videos of their children via social media, often associated with the oversharing of such images.

Smishing: SMS Phishing (*See phishing)

Spear Phishing: Targeted cyber attack on individuals or companies to steal sensitive data or install malware. Attackers pose as someone known to their target.

Trolling: Deliberately provoking or upsetting someone online to obtain a reaction.

VR: Acronym for Virtual Reality – an immersive 3-dimensional online experience.

Virus: A type of malware designed to cause harm to a computer system.

Vishing: Similar to phishing but using voice messaging or calls.

VPN: Acronym for Virtual Private Network – an encrypted network that can be used as a secure connection when using public internet.

Walled garden: A means of allowing only pre-approved content or websites.

Wiki: A website or page that allows users to contribute content.

XRW: Acronym for Extreme Right Wing. Online content associated with criminal activity motivated by Neo-Nazism, Racism, Fascism etc.

Additional Resources:

Glossary for internet safety and terms | Internet Matters

Internet & slang terms glossary | Internet Matters

Glossary of E-Safety Terms (e2bn.org)

Glossary - Get Safe Online

A-Z glossary of online terms | Technology and internet | Age UK

Internet-Safety-GlossaryA4_rev-4621_Edition-4.pdf (safeguardingpartnership.org.uk)

Appendix 2: Artificial Intelligence (AI)

Artificial Intelligence (AI) has been around for a while. It is already used to assist in several online tasks, for example: spam filters on email accounts, voice recognition software and support chatbots on websites. Its use is growing, and its capabilities are developing quickly. The question of how it will impact our lives into the future is a source of much speculation, excitement and concern.

An area of innovation that has particular implications for online safety is 'generative AI'. That is, the use of AI tools to create new content – this could be text, images, sounds or videos. As technology improves, the content generated by AI becomes more realistic and convincing. This opens up amazing opportunities for creativity and innovation, but also for the technology to be misused with the intent to deceive or cause harm.

In 2023, the Internet Watch Foundation (IWF) investigated its first reports of child sexual abuse material generated by AI. Their report states:

"Initial investigations uncovered a world of text-to-image technology. In short, you type in what you want to see in online generators and the software generates the image…These AI images can be so convincing that they are indistinguishable from real images."

It cites one key finding as:

"In total, 20,254 AI-generated images were found to have been posted to one dark web child sexual abuse material forum in a one-month period."

The creation, distribution and viewing of these images is illegal in the UK. These images cause harm to children because they can be based on children known to the perpetrator, children who are already victims of child sexual abuse and children in the public eye.

Generative AI can also be used to create plausible, targeted scam materials – increasingly convincing emails designed to replicate communications from reputable companies, for example.

So, what can we do to protect our communities?

- We can raise awareness about generative AI with vulnerable groups- encouraging people to pause and think whether what they encounter is genuine.

- Make sure everyone in our community knows to pass on concerns about anything worrying they encounter online.
- Report all harmful online material to the appropriate body (see signposting section of this handbook) and illegal activity to the police.
- Safely store all personal data and images.

Further information on AI in the context of online safety:

How AI is being abused to create child sexual abuse material (CSAM) online (iwf.org.uk)

The Children's Commissioner's view on artificial intelligence (AI) | Children's Commissioner for England (childrenscommissioner.gov.uk)

UNICEF-Global-Insight-policy-guidance-AI-children-2.0-2021.pdf

Appendix 3: Basic Cyber Security

There are several simple steps you can take to keep your organisation's devices and online activities safer from cyber-attacks and scams. Much of the information below would also be helpful to pass on to people in your community so they can protect their own devices and data.

Device safety tips

- Keep your devices locked so only you can use them and access your apps and accounts. Where available, set fingerprint or face ID.
- Protect your devices against viruses, malware and spyware. There are apps you can download to reduce the risks.
- Log out of apps when you finish using them, don't just close the screen – this is especially important for financial apps.
- Don't use 'free' public wi-fi to access your online accounts or send or check private or sensitive information – they can be hacked easily.
- Update your device. Always keep your device's operating system and apps up to date so you have the latest security features and bug fixes.
- Avoid saving passwords in your browser. This may be convenient, but it also means that anyone who has access to your computer or device can access your online accounts, such as bank, social media and email accounts.
- Remove or delete apps that you no longer use.
- Consider covering your device cameras for extra security. It's unlikely the camera can be turned on without your consent, but it is possible.
- Consider hiding the location of your devices by switching off location-based services, and decide whether or not you want photos and documents to be geotagged with your location.

- Regularly review your privacy and security settings to check they are best for your situation.

Websites:

- Use secure sites, i.e., those with 'https://' in the website address and a locked padlock icon in the browser.
- Log out of sites as soon as you have finished using them.
- Avoid signing into apps and websites with your social media account. When you use your social media account to sign into other apps or online accounts, you are often agreeing that this website is allowed to have access to all the information you share in your other account.
- Look closely at user agreements, terms and conditions, and disclaimers.
- Ignore optional information requests when completing online forms. Required information is usually marked with an asterisk (*).
- Look at reviews and customer satisfaction websites before buying from a site for the first time.
- Turn off, clear or delete cookies.

Email:

- When you receive an email, ask yourself- do I know and trust the person / organisation that sent this? Does the tone, word choice and spelling match what I would expect from them?
- Don't click on links or attachments you were not expecting, even if you think you know who sent them. Check the address carefully – if even one letter is different to the real address it's likely to be a scam.
- A common attack is an email that says your password has expired or your account is being updated – the email will then direct you to enter

your security details or sensitive information on a fake web page that may look very convincing.

- Remember, banks will not email you to ask for your account details.
- Watch out for courier messages, 'prizes', urgent requests, offers too good to be true, and warnings that you must provide security information if you don't want to get into trouble – they are often scams.
- Never provide sensitive security information via email.

Passwords and passphrases

- Set up strong passphrases and multi-factor authentication to secure important accounts, like those with financial information or health records.
- Do not choose the same password or passphrase for multiple devices, accounts or apps.
- Do not share passwords. Treat passwords and access codes for your devices like codes for your bank accounts – never share them with anyone.

Many of the tips above are adapted from this resource, where you can also find a lot of other useful information:

Further advice is available from:

National Cyber Security Centre - NCSC.GOV.UK

Keeping digital devices safe from malware - BBC Bitesize

How to stay safe online as an older person | Age UK

Appendix 4: Communicating with Under 18s

Safe and appropriate communication with children and young people is a safeguarding priority for all organisations working with under 18s. Our policies and codes of conduct need to include online communications as well as physical interactions so that staff, volunteers, parents, care-givers, children and young people, and the wider community, know what is expected.

Firstly, consider - do you need to communicate online with children and young people at all, or could this be done via parents/care givers?

If you do need to communicate online with under 18s, ensure there are at least two safely-recruited workers in the conversation for accountability. Preferably, communication will be via equipment provided by the organisation. If this isn't possible and staff and volunteers are using personal devices, this should only be done in line with your online safety policy.

Here are some good practice considerations you can apply to your context and include in your policy:

1. **Consider your purpose:**

- Make sure you are contacting the child for something related to the work of your organisation.
- Make sure your reason for communicating is clear and obvious to the child.
- Only use email, group messages etc to communicate specific information (e.g. times and dates of events) rather than as a relationship building tool.

2. **Consider your tone:**

- When communicating with children and young people, use an appropriate tone. Be warm and friendly, but not over-familiar or personal.
- Make sure your tone doesn't suggest or offer a special relationship. Remember, this isn't just about your intention, it's about how the child receives it.
- If your message was read by someone else, could there be any misinterpretation of your meaning or intentions?

3. **Consider what you share:**

- Don’t share any personal information with children, or request or respond to any personal information from a child, other than things appropriate as part of your role.
- On social media, make sure your privacy settings restrict children being able to see any more than what is relevant to communication within the group.

4. **Consider when you communicate:**

- In general, email/internet communication with children should take place in normal working hours (9am-5pm).
- Exceptions to this should have clear and valid reasons e.g. last-minute alterations to planned evening meetings when young people are on their way without parents.
- Online activities taking place outside of these hours should be planned in advance with parental consent.

5. **Consider social media:**

- Don’t make ‘friends’ with or ‘follow’ children and young people on social media.
- Make sure social media interaction between workers (paid or voluntary) and under 18s is limited to groups monitored/administrated by at least two safely-recruited workers.
- Any social media groups your organisation has for under 18s should be moderated by at least two leaders.
- Make sure the social media platforms you use have an appropriate minimum legal age for your group. For example, the minimum age for Facebook is 13, so this is not an appropriate platform if you are working with 11- and 12-year-olds.
- Use security settings to ensure that only the information you want to be visible is visible, limit who can see it, limit who can contribute etc.

6. **Consider accountability:**

- Generally, maintain good and open relationships with parents and carers regarding communication with them and their children. Explain when

and why and how you might want to contact under 18s and get parental consent to do so.

- Make sure there are at least two adult leaders monitoring all group chats, social media groups and online video activities with under 18s.
- Maintain records of all electronic contact with individuals or groups, including messaging and texting.
- If a child or young person makes contact with you online, tell your team leader / supervisor.

As always, if any online communication you have with a child makes you worried that they or someone else may not be safe, tell your safeguarding lead.

Appendix 5: Online Safety Act

The Online Safety Act became law in October 2023 and covers the whole of the UK. The Act is intended to ensure the safety of online users within the UK. This is a complex task as it covers not just companies operating, and content produced, in the UK but globally.

The law directly applies to businesses and organisations that offer online services such as websites, apps and other types of online platforms that are accessed within the UK, regardless of where the organisation is based.

Whilst the detail of the Online Safety Act is very complex, the main expectations for online service providers include:

- Assessing the risk linked to the use of their services, particularly access to harmful content
- Assessing the risk of harm to children from harmful content
- Taking effective steps to mitigate any risks identified in the risk assessment process
- Provide clarity of how the organisation assesses and protects against risk
- Have clear and easy to use systems to report concerns and illegal or harmful content
- Provide a clear and robust complaint system
- Consider the importance of rights to expression and privacy

The Law is being phased in over a period of time and many organisations are continuing to develop their responses.

Further information

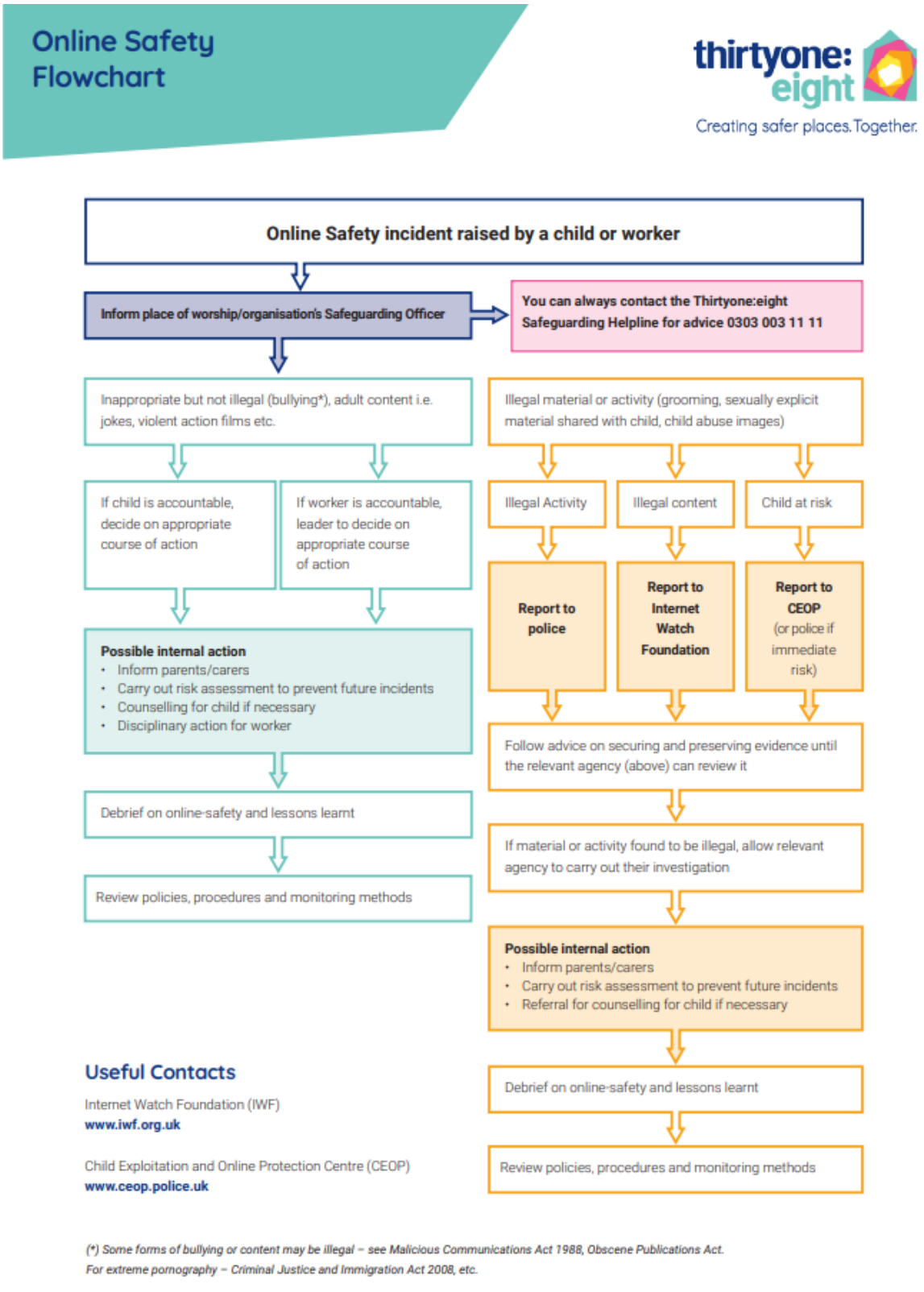
New rules for online services: what you need to know - Ofcom

Online Safety Act: explainer - GOV.UK (www.gov.uk)

The Online Safety Act: what it means for children and professionals | NSPCC Learning

Appendix 6: Online Safety Flowchart

This flowchart guides you through how to respond to an online safety incident. It is one of many safeguarding resources available in the Members' Area of our website:



Online Safety

Appendix 7: Online Pornography

Most adult pornography is legal in the UK. Pornography has also been around for much longer than the internet and is seen by many as a harmless way to fulfil sexual needs. Why, then, include a section about it in a course about online safety?

Pornography accounts for a huge amount of internet activity. A 2023 study showed that porn sites are visited more often than Amazon, Netflix, TikTok, Instagram, YouTube and other popular websites[4]. Research also shows that several aspects of online pornography have safeguarding implications:

Sexual Violence

A lot of the readily available content on mainstream sites includes acts of sexual violence. This can normalise abuse:

"1 out of every 8 porn titles shown to first-time users on porn site home pages describe acts of sexual violence."[5]

"At least 1 in 3 porn videos show sexual violence or aggression.[6]"

Impact on children

The ease and anonymity with which pornography is accessible online also makes it more likely that children will be exposed to it, compared to the time when it was purchased in newsagents or specialist shops:

"Most kids today are exposed to porn by age 13[7], with 84.4% of males and 57% of females ages 14-18 having viewed porn.[8]"

There are many reasons why children may watch online pornography. It's normal for young people to be curious. They might watch to explore new

[4] How Many People Actually Watch Porn? | Psychology Today

[5] Vera-Gray, F., McGlynn, C., Kureshi, I., & Butterby, K. (2021). Sexual violence as a sexual script in mainstream online pornography. The British Journal of Criminology, doi:10.1093/bjc/azab035

[6] Fritz, N., Malic, V., Paul, B., & Zhou, Y. (2020). A descriptive analysis of the types, targets, and relative frequency of aggression in mainstream pornography. Archives of Sexual Behavior, 49(8), 3041-3053. doi:10.1007/s10508-020-01773-0

[7] British Board of Film Classification. (2020). Young people, pornography & age-verification. BBFC. Retrieved from https://www.bbfc.co.uk/about-classification/research

[8] Wright, P. J., Paul, B., & Herbenick, D. (2021). Preliminary insights from a U.S. probability sample on adolescents' pornography exposure, media psychology, and sexual aggression. J.Health Commun., 26(1), 39-46. doi:10.1080/10810730.2021.1887980

feelings, to learn about sex and relationships, for a dare or a joke, or because of peer pressure. Online pornography can give children harmful messages and expectations about sex, consent, their bodies and relationships.

Link to harm and abuse of others

It is not only children's perceptions of healthy relationships that are affected by online pornography. The Lucy Faithfull Foundation published a report in 2024 drawing a link between viewing adult pornography and online sexual offending against children. It explains:

"Viewing pornography where the societal norms and rules of consensual sex are violated could have an impact on a person's perception of what type of pornography or sex is acceptable."[9]

Industry abuse and trafficking

As well as the impact on those watching it, the creation of online pornography can sometimes make people victims of abuse. It is very difficult for the viewer to know if this is the case:

"There have been many documented instances of verified accounts posting nonconsensual content, child sexual abuse material, or content made of sex trafficking victims."[10]

Help and support: If you are worried about the impact of pornography for yourself or someone else, there are some sources of further information and support below. If you have a safeguarding concern, tell your safeguarding lead and there are reporting mechanisms detailed in the signposting section of this handbook.

Fortify (app and website)

Naked Truth Project

Fight the New Drug

Screen Accountability™ | Covenant Eyes

Stop It Now | Preventing child sexual abuse

[9] 2024_05_Faithfull_Paper_Viewing_Pornography_Link_Final_Spreads.pdf (lucyfaithfull.org.uk)
[10] Pornhub sued by 40 Girls Do Porn sex trafficking victim. (2020). BBC News. Retrieved from https://www.bbc.com/news/technology-55333403 ParlVu. (2021). Meeting no. 20 ETHI— Standing committee on access to information, privacy and ethics.

Appendix 8: Risk of Suicide

When something has gone wrong within the context of the online world, this can be devastating for an individual. The understanding that 'once it is on the internet, it is there forever' is very daunting. We often use that phrase to deter people from putting inappropriate content online, but it can cause people to fear that there is no way to move forward positively.

When faced with an apparently hopeless situation, it is can cause people to consider ending their life through suicide. We need to ensure that we communicate that when online abuse takes place, there is hope and that things can be done to lessen the impact.

You may become aware that someone is considering taking their own life. It is important that you feel empowered to ask them about it and have a conversation where you can offer support.

A simple action plan would be:

- Recognise the risk
- Ask them about it
- Listen to them
- Show them you care
- Get emergency help if required
- Accompany them to safety

Resources for times of crisis:

SPUK - Suicide Prevention UK A range of support and advice for people in a crisis – contains helpful resources about a wide range of mental health conditions.

Papyrus UK Suicide Prevention | Prevention of Young Suicide (papyrus-uk.org) - support by text, email or phone for those thinking of suicide.

Samaritans | Every life lost to suicide is a tragedy | Here to listen 24/7 telephone support line

Zero Suicide Alliance (ZSA) - Resources for suicide prevention, including a free 20-minute online training course.

Shout: the UK's free, confidential and 24/7 mental health text service for crisis support | Shout 85258 (giveusashout.org) Free text service

I feel suicidal | Campaign Against Living Miserably (CALM) (thecalmzone.net) Helpful guides and helpline to help you provide support to those at risk of suicide. They provide a range of suicide prevention training.

Where to get urgent help for mental health - NHS (www.nhs.uk)

Stay Alive App - Grassroots Suicide Prevention (prevent-suicide.org.uk)

Appendix 9: Support for Parents and Carers

The focus of our webinar is on the awareness and actions needed for us to fulfil our organisational responsibilities in terms of online safety. However, many of us also want to support and equip the families in our communities outside of their contact with our organisation. This appendix identifies some key ways that parents and carers can help their children stay safe online and gathers together some useful resources to support them in this.

Set parental controls:

One way that families can enable their children to have safer online experiences is by setting parental controls on networks, apps, websites and devices. Internet.matters.org has a wide range of step-by-step guides to support parents and carers through this process.

Create a family agreement:

A family agreement about internet usage is a great way to start open conversations about online safety, as well as setting clear expectations and boundaries. Several organisations provide templates and guides for families who would like to create one:

Family Agreement | Childnet

Family Agreement template - Internet Matters

NSPCC Family Agreement

Keep having conversations:

Abuse thrives in secrecy. One of the best ways to keep children safe online is to have regular, open, age-appropriate conversations with children about what they are doing and experiencing online. Sometimes it can be difficult to know how to start or what to say. Here is some advice and guidance:

Five tips for talking about online safety with young children - UK Safer Internet Centre

Have a conversation | Childnet

How to talk to children about keeping safe online | Barnardo's (barnardos.org.uk)

Talking to your child about online safety | Parent Club

Teaching Your Child about Internet & Online Safety | NSPCC

Thinkuknow Jessie & Friends: film for parents and carers (subtitled) (youtube.com) Videos produced by the ThinkUKnow campaign in conjunction with CEOP. Introduces some basic online safety concepts for younger children through cartoons.

Stay informed:

Keeping up to date with all the various apps and platforms that children use can seem a daunting task. Here are some organisations that parents and carers can use to stay informed:

The National Online Safety App has free resources and regular updates for parents about popular apps, games, social media and messaging platforms.

Common Sense Media: Age-Based Media Reviews for Families this is a US-based resource that rates the suitability of the latest films, games, apps and TV shows for different age groups. It also has tips and FAQs for parents.

Online safety blog | NSPCC The NSPCC's online safety blog shares tips and advice for parents and carers, including articles such as: 'Is BeReal Safe for my child?', 'The influence of influencers' and 'Should I let my child use Discord?'

Online Behaviour & Safety | Parent Club Scotland's Parent Club has regularly updated advice and guidance searchable by age group.

Worried? Report your concern:

The primary way for parents and carers to respond if they or their children are worried about something they've encountered or experienced online is to support and reassure the child. Thank them for talking about it, affirm that it was the right thing to do and listen to their worries. The following resources give guidance about what to do if you are worried:

Get Support | Childline Various ways for children and young people to get support including helpline, video call with BSL interpretation, text and email.

Staying safe online | Childline Information about what to do if you are worried and online safety tips.

Get help for parents & carers | Childnet Includes information about where and how to report various types of online harm.

Child online safety: Top parental concerns | Internet Matters Tips and advice related to common parental concerns.

Signposting to other useful organisations and resources

Please note: These links are accurate at the time of course preparation. Thirtyone:eight don't recommend organisations, but you may find these links useful when looking for support and guidance.

Helplines for times of crisis:

Get Support | Childline Various ways for children and young people to get support including helpline, video call with BSL interpretation, text and email.

Find a Helpline (helplines.org) Helplines partnership is a database of helplines searchable by area of need.

Samaritans | Every life lost to suicide is a tragedy | Here to listen Free helpline available 24 hours a day, 365 days a year. You can also call the Samaritans Welsh Language Line on 0808 164 0123 (7pm–11pm every day).

National Suicide Prevention Helpline Uk » Home (spuk.org.uk) Helpline open 6 pm – midnight everyday 0800 689 5652

Papyrus UK Suicide Prevention | Prevention of Young Suicide (papyrus-uk.org) Papyrus Hopeline is available hours a day, every day 0800 068 4141 website has other ways to get in touch too.

Reporting online harm:

If you or someone else is at immediate risk of significant harm, call 999.

Action Fraud Report fraud and cybercrime in England, Northern Ireland and Wales. In Scotland, report to Police Scotland.

Action Counters Terrorism Report possible terrorism, radicalisation and violent extremism. Also here: Report online material promoting terrorism or extremism - GOV.UK (www.gov.uk)

Advertising Standards Authority Report an online scam advert or inappropriate online advert.

CEOP Safety Centre Report online child sexual abuse and grooming.

Internet Watch Foundation Report online child sexual abuse images and videos.

Report Harmful Content Report various types of online harms experienced on specific platforms.

Report Remove | Childline Under 18s can confidentially report sexual images and videos of themselves and have them removed from the internet.

Revenge Porn Helpline - 0345 6000 459 | Revenge Porn Helpline A UK service supporting adults (18+) who are experiencing intimate image abuse, also known as, revenge porn.

Stop Non-Consensual Intimate Image Abuse | StopNCII.org Resources and support for adults who have experienced financially motivated extortion.

True Vision Report hate crime (site owned by National Police Chiefs Council).

Keeping Children and Young People Safe Online:

BBC Bitesize - What is online safety? Resources and quizzes aimed at Key Stage 2 (7-11 year old) children.

Breck Foundation Charity giving advice and support relating to online child sexual abuse and grooming.

Childline - Online and mobile safety Information, support and resources for children and young people.

Childnet Resources, articles, advice and guidance. Separate sections for teachers and professionals, parents and carers, children and teens.

Common Sense Media: Age-Based Media Reviews for Families | Common Sense Media US resource useful for signposting parents. Reviews suitability of major games, films, TV shows and apps for different age groups.

Hwb (gov.wales) -Keeping safe online Welsh government online safety hub.

Internet Matters Guides, articles and resources searchable by age group and topic.

Marie Collins Foundation Organisation supporting children, families and their communities who have experienced online child sexual abuse.

NSPCC - Keeping children safe online Online safety information, research and advice from NSPCC.

Example online safety policy statement | NSPCC Learning Free template for an online safety policy and child / young person's agreement for organisations working with children and young people.

Parent Club Scotland - Online Behaviour & Safety Advice and guidance for parents and carers.

Parental controls & privacy settings guides | Internet Matters Searchable instructions for setting controls on a wide range of ISPs, devices and apps.

Parents Protect - Internet Safety Links Signposting to a wide variety of online resources for parents

Police Service of Northern Ireland - Online Safety | Information and advice from PSNI.

Safeguarding Board for Northern Ireland (SBNI) Online Safety Hub Information and advice from SBNI, covers adults and children.

SmartSocial.com US-based YouTube channel for parents, carers and people working with young people. Advice and resources about safe use of social media.

UK Safer Internet Centre National charity including helplines for professionals working with children and young people, reporting mechanisms, guides, resources, training, research and materials to deliver annual Safer Internet Day sessions.

The Upstream Project | Stop It Now! Scotland | Prevent Preventing child sexual abuse online in Scotalnd.

Youthscape Christian youthwork charity. This link goes to one of many articles they have around how the online world impacts young people. They also partnered with us to create this guidance for online youthwork.

Also, National Online Safety app, available on all devices. Info here .

Keeping At-Risk Adults Safe Online:

Age UK - Beginner's Guide to Online Safety Practical and straightforward guidance booklet about online safety aimed at older adults. It includes how to

recognise various types of online scams and information about banking and shopping safely.

Age UK - How to stay safe online as an older person Age UK's webpage about online safety including WhatsApp, social media, protecting devices, password security etc.

Ann Craft Trust - How to Stay Safe Online - Guidance for Adults and Young People with Learning Disabilities - Digital Safeguarding A collection of information guides for people with learning disabilities. Guides use simple language and pictures to aid understanding.

Foundation for People with Learning Disabilities - Staying Safe on Social Media and Online Free download easy read guide to online safety for people with learning disabilities/

Mencap - Bullying Online Information about online bullying and links to further resources about online safety.

Supporting Vulnerable Groups Online - UK Safer Internet Centre Advice and resources for anyone working with vulnerable groups.

Regulation and Information:

Information Commissioner's Office (ICO) The ICO is a public body that protects data privacy and freedom of information. It has offices in all 4 UK nations. A current focus of their research and regulation is Artificial Intelligence (AI).

National Cyber Security Centre - NCSC.GOV.UK National body to protect UK from cyber threats – includes information for organisations and individuals about cyber security.

Ofcom Ofcom is the communication services regulator. Their website has lots of information about online safety and they publish annual research reports on media usage for children and young people (see below):

Children and parents: media use and attitudes report 2024 – interactive data - Ofcom Searchable data about media use and attitudes to highlight statistics and trends.

Children Media Lives 2024 (ofcom.org.uk) Long running qualitative research survey talking to a variety of children and young people about their media usage.

UK Council for Internet Safety - GOV.UK (www.gov.uk) The UK Council for Internet Safety (UKCIS) is a collaborative forum combining government, the tech community and the third sector. They publish policy, research, advice and guidance.

UKCIS_Digital_Resilience_Framework.pdf (publishing.service.gov.uk) Published by the UK Council for Internet Safety. This is a framework and tool for organisations, communities and groups to help people build resilience in their digital life.

UK National Policies:

Online Media Literacy Strategy - GOV.UK (www.gov.uk) This strategy sets out the UK government's plan to empower make safe choices online through media literacy education.

Online Safety Strategy and Action Plan | Department of Health (health-ni.gov.uk) This is the strategy for Northern Ireland. Its aim is to educate and empower children and young people online.

Internet safety for children and young people: national action plan - gov.scot (www.gov.scot) This is the action plan for Scotland. Its aim is to ensure there are frameworks for training, support and information for professionals, families, children and young people.

Enhancing digital resilience in education: An action plan to protect children and young people online - Hwb (gov.wales) This is the action plan for Wales. The aim is to help protect children and young people from illegal, harmful and false content on the internet and to promote safe, responsible and considerate behaviour online.

Tackling Child Sexual Abuse Strategy - GOV.UK (www.gov.uk) In England and Wales, the tackling sexual abuse strategy addresses abuse both off and online.

Links commonly used throughout the webinar

Please note: As above, these links are accurate at the time of course preparation. Thirtyone:eight don't recommend organisations, but you may find these links useful when looking for support and guidance.

These are shared in the order they're likely to be mentioned during our webinar. Some of these are also included in our signposting section.

Introduction:

www.charitycomms.org.uk - Source of course aim quote

Children and parents: media use and attitudes report 2024 – interactive data - Ofcom – Source of childhood statistics

www.ageuk.org.uk – Source of older adult statistic

www.ofcom.org.uk – Source of UK time online statistic

https://doi.org/10.21241/ssoar.71817 - Original source of 4 'C's: Livingstone, S., & Stoilova, M. (2021). The 4Cs: Classifying Online Risk to Children.

Content:

www.iwf.org.uk/annual-report-2023

International Scientific Report on the Safety of Advanced AI - GOV.UK (www.gov.uk)

BBC Radio 4 - File on 4, Degraded by Deepfakes

Government cracks down on 'deepfakes' creation - GOV.UK (www.gov.uk)

BBC Radio 4 - File on 4, The Murder of Brianna Ghey - A File On 4 special

Holly Willoughby targeted by kidnap, rape and murder plot - court - BBC News

Hate crime | Cambridgeshire Constabulary (cambs.police.uk)

Hate crime, England and Wales, 2021 to 2022 - GOV.UK (www.gov.uk)

Who is Andrew Tate? The self-proclaimed misogynist influencer - BBC News

Education Resources - UK Safer Internet Centre

Example online safety policy statement | NSPCC Learning

Parental controls & privacy settings guides | Internet Matters

Contact:

www.iwf.org.uk/news-media - Source of quote from Susie Hargreaves

Online safety blog | NSPCC

Conduct:

saferinternet.org.uk/online-issue/cyberflashing

'It can happen to any child': parents of sextortion victim send out warning | Children | The Guardian

Report Remove | Childline

www.ceop.police.uk/safety-centre

Commerce:

www.actionfraud.police.uk Action Fraud online or 0300 123 2040

Forward any suspicious emails to: report@phishing.gov.uk The National Cyber Security Centre (NCSC) will investigate them.

If you receive suspicious text messages, forward them to 7726 (it's free). This will report the message to your mobile phone provider.

How to manage your digital safety settings | eSafety Commissioner

11 practical ways to keep your IT systems safe and secure | ICO