Online Safety Practice Guidance & Procedure

Fostering, Adoption & Children's Services

As part of Polaris community, the term 'foster parent' is preferred but it is recognised that 'foster carer' is also used in legislation and within the community.

The term 'child' or 'children' is used to refer to all children under the age of 18 years (where the context specifically relates only to older children, the term 'young person' is used).

This procedure forms part of the Polaris Community Quality Management System in line with ISO-9001:2015 standards and applies to all companies within the Community unless stated otherwise.

Procedure Owner:	Quality Assurance and Safeguarding Team
Approved by:	Head of Safeguarding
Date approved:	Sept 2025
Next review date:	Sept 2028
Version No:	03

Contents

Introduction

We are committed to supporting children to explore the digital world safely. Through active monitoring, education, and engagement, we aim to reduce risks associated with new and emerging platforms while promoting trust, independence, and digital resilience.

This procedure reflects legal duties under the **Online Safety Act 2023**, which aims to make the UK the safest place in the world to be online. It is also aligned with the principles set out in the Children Act 1989, the Data Protection Act 2018, and the GDPR to ensure compliance with current child safeguarding and data protection laws.

The **Online Safety Act 2023** places duties on social media platforms and internet services to:

- Remove illegal content (e.g., child sexual abuse material, terrorism, hate speech).
- Prevent children from accessing harmful content (e.g., suicide, self-harm, pornography).
- Require age verification for certain content.
- Make it easier for users to report harm and access safety tools.

While enforcement lies with **Ofcom** children's service providers must ensure internal safeguarding procedures align with the Act's aims.

Definitions of Online -Safety

Online safety refers to the practice of protecting children, young people and adults from risks and harms associated with using the internet, digital devices, and online technologies. This includes risks from:

- Inappropriate or harmful content
- Exposure to pornographic images via the internet.
- Online grooming and exploitation
- Cyberbullying and harassment
- Sharing personal or sensitive information
- Sexting and Non-Consensual Image Sharing
  e.g., sharing sexual images or videos, especially involving children or without consent
- Exposure to radicalisation, extremist ideologies, scams, or misinformation
- Offensive material and websites, including those promoting harmful coping strategies, such as self-harm, suicide and eating disorders.
- Excessive screen time and digital addiction e.g., compulsive use of games or social media affecting wellbeing, sleep, schoolwork, or social interaction.

Children who have experienced past trauma, or who have low self-esteem, can be more vulnerable to the dangers associated with being online and will need support to learn about online safety. In addition, foster/adoptive parents will need support and guidance to recognise and respond appropriately to online risks that children may face.

Perpetrators of online sexual abuse often use social networking sites as an easy way to access children and young people. In addition, radical and extremist groups may use social networking to attract children and young people into rigid and narrow ideologies that are intolerant of diversity or promote extreme behaviours and justify or attempt to justify political, religious, sexist or racist violence.

Risks to children

The above listed risks that children face online are commonly split into the following categories:

content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.

It is important that those who care for children consider the safety and reliability of online material and be aware that information may be harmful, misleading, and written with a bias.

contact: being subjected to harmful online interaction with other users, for example, peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

Children may be contacted online by individuals who seek to groom them into sexual activity. Online harm may also include online bullying (often referred to as '*cyberbullying'*. This is when a child is tormented, threatened, harassed, humiliated, embarrassed, or otherwise targeted by another child or adult using the internet or mobile devices. It is possible for one victim to be bullied by many perpetrators.

conduct: online behaviour that increases the likelihood of, or causes, harm to children or others. for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.

Children need to be aware of the impact that their online activity can have on both them and other people, and the digital footprint that they create on the internet. Children may share personal information and take risks such as chatting to strangers or sharing sexual images (youth produced sexual imagery, often referred to as 'sexting'). Alternatively, they may bully or intimidate others.

Youth produced sexual imagery/'sexting' describes the use of technology to generate images or videos that are of a sexual nature and are indecent. The content can vary, and includes nude or partially nude images, and videos of sexual activity. These images are shared between children (and sometimes adults) and often with people they may not even know. Children are not always aware that their actions are illegal, and the use of smart phones has made the practice much more commonplace. It is illegal to make, possess and distribute indecent images of children under the age of 18.

Commerce: - illegal, inappropriate, or harmful online commercial activities that can compromise the health and wellbeing or security of children or others. Risks such as online gambling, inappropriate advertising, phishing and or financial scams.
Children can be unaware of hidden costs and advertising - Children may not be aware of the hidden costs of 'in-app purchases' or subscription purchases and can create significant unexpected bills when their purchases are linked to a credit card or phone contract.

Social networking apps are also widely used as an advertising tool for companies, and children are frequently targeted by adverts. Online 'influencers' with a target audience of

children will also advertise products for a fee but not always disclose this fact. Children can therefore be subject to social influence and pressure to conform to a perceived social norm.

Sextortion (Sexual Extortion)

What is Sextortion?

Sextortion is a form of **online sexual exploitation** where an individual is threatened or coerced into sharing explicit images, videos, or engaging in sexual activity online. It typically involves a perpetrator gaining trust, obtaining sexual content, and then threatening to distribute it unless further material, money, or sexual favours are provided.

This exploitation can occur through:

- Social media platforms
- Messaging apps
- Online games
- Video calls or livestreams
- Fake online profiles ("catfishing")

Perpetrators often impersonate peers, celebrities, or romantic interests to gain trust.

Why Children and Young People Are Vulnerable

Children and young people may be particularly vulnerable to sextortion due to:

- Curiosity or experimentation
- Lack of awareness of online risks
- Pressure to conform to peer expectations
- Grooming and manipulation by offenders
- Emotional blackmail and fear of getting into trouble

Those with lower self-esteem, limited adult supervision, or prior trauma may be at increased risk.

Warning Signs of Sextortion

- Withdrawal or secrecy around device use
- Sudden anxiety or fear related to being online
- Emotional distress after using social media
- Demands for money or privacy from the child
- Attempts to delete accounts or messages
- Reluctance to discuss online interactions

Preventive Measures

- Discuss the risks of sharing images online in a non-judgmental way.
- Emphasize that no one should ever pressure them to share sexual content.
- Reassure children they will not be punished for speaking up.
- Use privacy settings and disable direct messages from strangers.
- Encourage children to report inappropriate behaviour immediately.
- Ensure children understand consent, coercion, and reporting mechanisms.

Responding to Sextortion

If a child discloses or you suspect sextortion:

1. **Stay calm and listen** without blame or judgment.
2. **Do not delete messages or images**—preserve evidence where possible.
3. **Do not confront the perpetrator.**
4. **Report the incident** to the Supervising Social Worker or equivalent and LA Social Worker
5. **Involve CEOP** (Child Exploitation and Online Protection Command) or the **police** if there is a risk of ongoing harm or criminal activity.
6. **Provide reassurance** and support for the child's emotional well-being.

See also: (Help if you're worried about 'sextortion' or online blackmail).
Sextortion - UK Safer Internet Centre

Risk Assessment

It is important that risk assessments are balanced and take into account strengths as well as areas of risk and vulnerability, therefore assessments should also include;

- Opportunities for positive online engagement, learning, and connection, including how the child uses the internet to explore hobbies, maintain friendships, or access support.
- The child's existing knowledge, digital skills, and ability to make safe choices online, and how these can be built upon through education and trusted adult relationships.
- Specific technology that the child will have access to.
- Agreed family rules about access and usage of technology and devices (e.g. where in the house they can be used and when).
- Any known history or current harm and agreed actions to manage any risk of harm.
- The online contact that children may have with their birth family.

If required, as part of the risk assessment, foster/adoptive parents will regularly check:

- Installed apps, social media platforms, and gaming accounts.
- Privacy settings, location sharing, and direct messaging features.
- Behavioural signs of distress or secrecy related to device use.
- Use **age-appropriate parental controls** and tools like screen time limits or app blockers.

NB: Detailed guides for applying parental controls on different home devices can be found at www.internetmatters.org/parental-controls.

NB: It is easier to install and monitor parental control software on shared family devices rather than a device owned by a young person. If a child comes to placement with their own device, the use of parental controls should be discussed and agreed with the local authority immediately.

NB: Be aware that adding children to a 'family' group for parental controls can result in problems removing the child from the group when they leave your family. Apple and Playstation do not currently permit the removal of a child's account from a family group. Before using this parental control option, families should discuss the implications and agree a plan of action.

⚠ **Note**: Platforms such as TikTok, Snapchat, and Discord pose specific risks including anonymous contact, disappearing messages, and unmoderated content. Any use of these should be reviewed regularly.

Preventing Online Harm

It can be difficult to find the balance between allowing children to reap all the benefits that technology offers and keeping them safe. We cannot prevent children from ever being exposed to online risks, so we must educate them about risks they may face, how to keep themselves safe and stress the importance of telling somebody if they have any concerns or worries.

It is very important that adults who care for children know enough about technology and the associated risks, to be able to advise children about their safety online.

Supervising Social workers or equivalent should:

- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Discuss online safety with foster/adoptive parents, and young people.
- Identify online safety concerns and take appropriate action by following the agency's safeguarding policies and procedures.
- Take personal responsibility for professional development in this area.

Foster/adoptive parents should:

- Encourage open conversations with the child about their online interests, friendships, and positive experiences, building trust and shared understanding.
- Recognise and praise safe and responsible digital behaviour, reinforcing the child's strengths and growing independence online.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Establish family rules about acceptable use of the internet and review these regularly, in partnership with children's social workers and with the help of their supervising social worker or equivalent.
- Take reasonable steps to monitor and supervise children and young people's online activities, in accordance with steps agreed in the child's individual Risk Assessment.
- Allow children to have age-appropriate access to the internet and mobile phones. Families are expected to have a computer at home that young people can use, with age-appropriate parental controls installed, and home internet access (with age-appropriate filtering in place). Mobile phones provided for young people must have appropriate and agreed parental controls installed.
- Role model safe and appropriate use of technology and social media.
- Identify changes in behaviour that could indicate a child is at risk of harm online, and share these concerns with their supervising social worker or equivalent.
- Seek help and support from the agency if they or their child experiences risks or concerns online.
- Take responsibility for their own awareness in relation to risks and opportunities posed by new and emerging technologies.

Engaging and educating children and young people

Children should be involved in discussions around e-safety expectations, privacy settings, and parental controls, in a way that is age-appropriate and promotes autonomy while maintaining safety.

Children and young people (at a level that is appropriate to their individual age, ability and vulnerabilities) should be taught, supported and encouraged to:

- Talk and learn about online safety.

- Follow the family's rules about the use of internet and mobile phones, both at home and when out in the community.
- Respect the feelings and rights of others, both online and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if they have a problem online, and support others that may be experiencing online safety issues.

Discussion with children about online safety should begin at the start of placement, including discussing and agreeing family rules about the use of the internet and technology. Family rules should consider:

- Time limits
- The types of website/specific websites that children are permitted or not permitted to use;
- Agreement for children to explain or show an adult what they are doing online;
- Any behaviour that is unacceptable online, e.g. bullying;
- Agreement to any privacy settings for social media accounts;
- Agreement for children to tell an adult if they are concerned about anything they see online;
- Agreement for children to ask before visiting a new website, and before setting up an account on a website or app.

Children should be supported to access the CEOP Education website and advised how they can contact CEOP (Child Exploitation and Online Protection Command) if they need to.

Safer use of technology

While children's access to the internet/specific websites might be prevented or withdrawn as a safeguarding measure, this should not be a permanent arrangement. Children need to learn how to use the internet and take responsibility for their own safety. This is best achieved by providing support in the home environment while accessing the internet.

The internet, mobile data and Wifi

- Foster/adoptive parents should consult with their internet service provider about age-appropriate filters to protect against the viewing of inappropriate material online, and apply the necessary restrictions.
- When young people have mobile devices with mobile data, the foster/adoptive parent/ should consult with the phone provider to identify any filters that can be applied.

Computers and laptops

- Foster/adoptive parents should have a home computer that young people can access for intenet use.
- Children should have their own restricted user account on the computer. This enables the application of different parental controls for different children, according to their age and personal vulnerabilities. Restrictions should be agreed with the supervising social worker or equivalent and the child's local authority social worker, and documented in the child's individual Risk Assessment.
- Computers should be positioned in shared family areas to facilitate appropriate monitoring of online activity. Children should only access the internet in their bedrooms if specifically directed by the local authority social worker.

Mobile phones and tablets

- Children's mobile phones and tablets should have age-appropriate parental controls applied. The extent of these controls should be agreed with the supervising social worker or equivalent and the child's local authority social worker, and documented in the child's Risk Assessment.
- Mobile phones and tablets can safely connect to the home internet service, if the necessary filters have been applied (see Wifi above).
- Mobile phones should not be kept in the child's bedrooms overnight, unless specifically directed by the local authority.

Gaming consoles

- Gaming consoles such as PlayStation and Xbox are Wifi enabled.
- The parental controls function can disable internet access, block or restrict apps and games to control adult-rated content. The extent of the controls applied should be agreed with the supervising social worker or eqivalent and the child's local authority social worker, and documented in the child's Risk Assessment.
- Gaming consoles should be positioned in shared family areas to facilitate appropriate monitoring of their use.

Safeguarding Children in Virtual Reality (VR)

As the use of VR and digital worlds (like the Metaverse) becomes more common, there may be additional risks to children (e.g., virtual bullying, inappropriate content, grooming). These emerging technologies require further consideration and risk assessment. To minimise risk:

Age Restrictions and Access

- Ensure children are **not using VR platforms below the recommended age**. For example, Meta Quest is not recommended for under-13s.
- Use **parental controls** to limit access, restrict purchases, and manage app usage.

Supervise Use

- VR should be used **in shared or supervised spaces**, not behind closed doors.

Phishing scams, **impersonation**, and **fraudulent messages**

Children and young people are increasingly targeted through **phishing scams**, **impersonation**, and **fraudulent messages**, especially via gaming platforms and messaging apps. These scams often involve:

- **Fake messages** that appear to come from trusted contacts or companies, asking for personal information, passwords, or payment details.
- **Impersonation of friends or online influencers** to build trust or encourage risky behaviour.
- **Clickbait links** offering free in-game currency, prizes, or exclusive content, which may lead to malware or data theft.

Children should be taught to:

- Never click on suspicious links or open attachments from unknown sources.
- Verify who they are talking to, even if the message seems familiar.
- Tell a trusted adult immediately if something doesn't feel right online.

Safer social networking

The term 'social networking' refers to use of social media apps and websites that promote connections, conversations and image sharing between friends and acquaintances.

To support safer social networking:

- Foster/adoptive parents and young people must not post things that might be considered threatening, hurtful, offensive or defamatory to others.

- Foster/adoptive parents must not post photographs of children online without the permission of the local authority and the child themselves. Any photographs stored digitally must be stored securely, in accordance with data protection law. Consideration should be given to safer caring plans for families and the children living with them.
- Foster/adoptive parents and young people should not connect with agency staff on social networking sites (unless they have a pre-existing friendship outside of fostering, of which the Registered Manager is aware).
- Foster/adoptive parents must not connect with children's birth family members on social networking sites.
- Foster/adoptive parents may connect with the young people they are looking after on social networking sites, but not with young people cared for by other families.
- Foster/adoptive parents are advised to log out of social media apps and websites after use, to ensure they are not used by others.
- Additionally in Fostering; children, young people and parents in Parent and Child Placements are educated about the rights of privacy of those living in the family household and not taking photographs without the awareness of those in the photographs. Photographs of fostering family household members should not be shared on social media or provided to other persons.

Foster/adoptive parents are encouraged to read 'parent guides' to social media sites. These are available on the NSPCC website.

Young people's social media use should be discussed and agreed with the local authority social worker and any monitoring expectations discussed and documented in the Risk Assessment.

Young people should be taught about safe and appropriate social networking in the home environment. They should be advised as follows:

- Consider the benefits and risks of sharing your personal details on social media sites which could identify you or your location. Examples include your full name, address, phone number and school you attend.
- Only approve and invite known friends on social media sites and deny access to others by making your profile private.
- Tell a trusted adult if someone contacts you online who is not meant to (this may include strangers or members of your birth family). Do not respond or accept them as a friend.
- Don't arrange to meet online-only friends in real life without permission, and only with a trusted adult present.
- Use secure passwords, and don't share them.
- Use social media sites that are appropriate for your age and abilities.

- Learn how to block unwanted contact and how to report problems.

Monitoring and Assessing Risks on Newer Digital Platforms

To safeguard children from potential harms on newer and rapidly evolving online platforms (e.g., TikTok, Snapchat, Discord), the following steps should be taken:

1. **Ongoing Risk Identification**
    - Regularly review the features of new and popular platforms, focusing on:
        - Direct/private messaging
        - Disappearing content (e.g., Snapchat stories)
        - Live streaming and video sharing
        - User anonymity and public chat servers (e.g., Discord)
    - Stay informed via online safety resources (e.g., Internet Matters, NSPCC, UK Safer Internet Centre).
2. **Device and App Monitoring**
    - With the child's knowledge and in line with care agreements, check devices for:
        - Installed apps and usage patterns
        - Privacy and safety settings
        - Signs of concerning behaviour (e.g., secretive use, sudden emotional changes)
        - See previous information in this procedure on use of parental controls and safety settings.

Responding to incidents of online harm

Children sometimes feel unable to tell an adult about an online concern they have, because they worry that their computer or phone will be removed from them, to 'keep them safe'. They also worry that they will get into trouble.

The way adults react to the knowledge that a child may be at risk, or have been exposed to concerning material online, is therefore very important.

Children should be supported to be familiar with the *Click CEOP (*Child Exploitation and Online Protection Command) button and know that they can report directly to CEOP if they are worried and do not feel that they can tell an adult. CEOP will help them to tell their trusted adults. CEOP advise that adults take care to avoid 'victim blaming' language when managing incidents of online harm to promote the child's recovery.

All concerns should be reported to the Supervising Social Worker (or the Out of Hours Social Worker) or equivalent who should discuss the issue with their line manager or the Registered Manager.

Concerns might include:

- Talking with unknown people online
- Using anonymous chat sites
- Online bullying
- Viewing pornographic or extremist material online

If a foster/adoptive parent or staff member is concerned that a child may be at risk online, or may have been exposed to inappropriate material, they must be advised to:

- Stay calm, and not to over-react or get angry or upset.
- Inform their supervising social worker or equivalent. The agency will notify the child's social worker of the issue and discuss appropriate action to take.
- Save any evidence there may be, ideally by removing the device and preserving the information on it. If this is not possible, taking screenshots is advisable for concerns about bullying, intimidation, radicalisation, grooming and so on, but screenshots must not be taken of any indecent images of children or adults. In the case of apps such as 'Snapchat', taking screenshots quickly will be the only way to preserve evidence.
- An immediate risk to the young person's safety may need to be reported to the Out-of-Hours service. This may include concerns of sexual exploitation, or potential criminal activity. The agency will initiate local safeguarding procedures.
- Any concerns in relation to a child's use or exposure to social media should be considered in accordance with the agency's Notifiable and Monitoring Events procedure.

Report it

A number of organisations and providers have specific "report it" functionality to tackle online abuse. Staff, foster/adoptive parents should report any concerning activity to the appropriate bodies and providers.

- If you have **concerns about online 'grooming'** or other concerning activity towards achild, then in an emergency, you must call 999, but otherwise report the activity to the child's social worker, and agree who will notify CEOP (Child Exploitation and Online Protection Command).
- If you have concerns about **illegal content** (in the UK that includes child sexual abuse images / obscene adult content then this must be reported to *The Internet Watch Foundation* (an independent not-for-profit organisation that works to stop

child sexual abuse online) and the police.

- Online **terrorism activity** must be reported to the police's Counter Terrorism Internet Referral Unit. A 'Channel' referral should also be made as part of the 'Prevent' programme.
- Suspected online terrorist material should be reported through contact with the police and https://www.gov.uk/report-terrorism.
- Online content which incites hatred on the grounds of race, religion, disability,sexual orientation or sex, should be reported to the police. The True Vision (a reporting function for hate crimes owned by the police) has a referral function.
- Online scams can be reported to Action Fraud.
- If you have a concern that foster/adoptive parents, or a member of staff may have acted inappropriately towards a child, or may have accessed material that depicts harm to a child, you must refer to and follow the relevant Safeguarding Procedures. See also Whistleblowing procedure.

Training, Information and Advice

The agency will provide training in online safety and online harms for staff, foster/adoptive parents. In addition, information and advice is readily available from a range of organisations:

www.thinkuknow.co.uk
www.childline.org.uk
www.internetmatters.org
https://reportharmfulcontent.com/
https://www.getsafeonline.org/
https://www.nspcc.org.uk/keeping-children-safe/online-safety/
Detailed guides for applying parental controls on different home devices can be found at www.internetmatters.org/parental-controls.

Review Dates:

June 2025 - Routine Review - additional detail added re Online Safety Act 2023**,** Virtual Reality and emerging technologies.
September 2025 - Minor update in line with KCSIE 2025 to Risks to Children section