E-Safety Practice Guidance Procedure

Fostering, Adoption & Children's Services

This procedure applies to the following agencies: Foster care Associates (FCA,) Foster Care Associates Scotland (FCAS), Fostering People, Orange Grove Foster Care, Clifford House Fostering, ISP, Foster Plus, ACS, AFA & Polaris Children's Services. The term 'agency' used throughout the procedure refers to these individual agencies.

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.

This procedure provides guidance in relation to e-safety and keeping children safer on line.

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.

The term foster parent is preferred but it is recognised that foster carer is also used in legislation and within the community.

Procedure Owner:	Quality Assurance and Safeguarding Team
Approved by:	Operations Board
Date approved:	20th July
Next review date:	July 25
Version No:	Replaces all existing versions

Contents

Definitions of E-Safety

Online safety or E-Safety are generic terms that refer to raising awareness about how children, young people and adults can protect themselves when using digital technology in the online environment.

The internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life. Children should be empowered to build resilience and develop strategies to manage and respond to risk online. However, children who have experienced past trauma, or who have low self-esteem, can be more vulnerable to the dangers associated with the internet and will need support to learn about online safety. In addition, foster parents and prospective adopters will need support and guidance to recognise and respond appropriately to online risks that children may face.

'Online harm' includes the following:

- Abusive images of children.

- A child or young person being groomed for the purpose of sexual abuse.
- Exposure to pornographic images via the internet.
- The use of the internet, in particular social media sites, to engage children in extremist ideologies.
- Offensive material and websites, including those promoting negative lifestyle choices such as self-harm, suicide and pro-anorexia.
- The use of the internet to threaten, harass, bully and humiliate children and young people (e.g. cyber bullying and relationship abuse).

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 risks children face online are commonly split into a number of categories:

Content: ***Age-inappropriate or unreliable content being available to children***

Children may encounter online content that is pornographic, violent, or extremist, or that promotes self/harm suicide or anorexia. 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.

Conduct: ***Children may be at risk because of their own behaviour, for example, by sharing too much information***

Children need to be aware of the impact that their online activity can have on both themselves and other people, and the digital footprint that they create on the internet. Young people 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 young people (and sometimes adults) and often with people they may not even know. Young people are not always aware that their actions are illegal and the increasing 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.

Contact: ***Children can be contacted by bullies or people who groom or seek to abuse them***
Children may be contacted online by adults 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.

Commercialism: ***Young people can be unaware of hidden costs and advertising***
Young people may not be aware of the hidden costs of 'in-app purchases' or subscription purchases and can create significant unexpected bills for parents/carers 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 young people are frequently targeted by adverts. Online 'influencers' with a target audience of young people will also advertise products for a fee but not always disclose this fact. Young people can therefore be subject to social influence and pressure to conform to a perceived social norm.

Risk Assessment

All risk assessments should include the measures taken to enable the child to use social media and the internet safely and to protect them from online harm.

The child's risk assessment should be informed by:

- Specific technology that they 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).
- Agreed use of privacy settings for social networks and online activity.
- Installation of parental control tools and how to use them.
- 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.

The use of monitoring and parental controls to prevent online harm should be in response to clearly-identified risks and proportionate to the risk. Parental control software allows an individualised approach to risk management.

Preventing Online Harm

It can be difficult to find the balance between allowing children to reap all the benefits that technology offers them, 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.

Agency social workers and support workers 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 parents, prospective adopters 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 parents/prospective adopters should:

- 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.
- Discuss online safety issues with children and reinforce appropriate, safe online behaviours at home.
- 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

i. 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.

ii. 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.

iii. 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.

i. The internet, mobile data and Wifi

- Foster parents and prospective adopters 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 parent/prospective adopter should consult with the phone provider to identify any filters that can be applied.

ii. Computers and laptops

- Foster parents and prospective adopters 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.

iii. 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.

iv. 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.

N.B. 1 Detailed guides for applying parental controls on different home devices can be found at www.internetmatters.org/parental-controls.

N.B. 2 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.

N.B. 3 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 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.

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. This may include blogs, forums, video sharing sites, chatrooms and messenger services.

There are a number of steps that can be taken to protect your privacy and reputation when using these sites and we recommend that all children, young people and adults follow them:

- Apply privacy settings to limit access to personal details, private thoughts, photographs and messages.
- Do not post things that might be considered threatening, hurtful, offensive or defamatory to others.
- Foster parents and prospective adopters 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 parents, prospective adopters 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 parents and prospective adopters must not connect with children's birth family members on social networking sites.

- Foster parents and prospective adopters 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 parents and prospective adopters are advised to log out of social media apps and websites after use, to ensure they are not used by others.
- Additionally 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 parents and prospective adopters 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 children's online activity

Families should take reasonable steps to monitor internet use within the home. This can be achieved by:

- Placing the computer/gaming device in a shared area so that the screen is visible to other people.

- Using parental control apps to restrict online activity and/or see what young people have been doing online.
- The extent of monitoring required will vary according to the child's age and personal vulnerabilities. Monitoring requirements should be discussed with the child's local authority social worker and agreed in the Placement Plan and the individual Risk Assessment.

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 parent, prospective adopter 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 parents and prospective adopters 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 parents, prospective adopters 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 e.g. Managing Allegations against Foster Parents /

prospective adopters, staff or the Whistleblowing Procedure as appropriate.

Training, Information and Advice

The agency will provide training in online safety and online harms for staff, foster parents and prospective adopters. 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/