Staying Safe Online

Policy and Guidance

Contents

1.0 Purpose 1
2.0 Scope 1
3.0 Policy Statement 2
3.1 Responsibilities 2
4.0 Guidance 3
4.1 Understanding the Risks 3
5.0 How to help children, young people and adults we support stay safe 6
5.1 Managing Access 6
5.2 Setting Boundaries 7
5.3 Communication and Involvement 7
5.4 Security and Privacy Controls 7
6.0 Responding and Reporting 8
6.1 Foster Carers 9
6.2 Residential Care 9
6.3 Schools 9
7.0 Procedures 9
8.0 Helpful Resources 9

1.0 Purpose

Outcomes First Group places the safety of the children and adults it supports as its highest priority. The purpose of this document is to set out the Group's policy for online safety and provide guidance to help keep the people it supports safe online and when using digital devices.

2.0 Scope

This policy applies to all of the Group's services and agencies operating in England, Wales, Scotland and Northern Ireland. It is applicable to fostering, residential care and schools.

This policy and guidance document should be read in conjunction with the Group's:

- Safeguarding Children & Young People Policy
- Child Exploitation Policy and Guidance
- Countering Bullying Policy and Guidance
- Adult Safeguarding Policy
- Images of Children Policy

3.0 Policy Statement

The Outcomes First Group is committed to keeping the children, young people and adults we support, educate and care for safe, whilst enabling them to enjoy their lives and have the same opportunities to explore the world as others.

Technology is part of everyday life for children and adults; it directly or indirectly affects almost every aspect of life. This provides many possibilities, including tools for learning, socialising, playing and helping young people find their place in the world. However, it also carries significant risks to which the children and adults we support can be more susceptible than their peers. Those already at risk offline are more likely to be at risk online.

Raising awareness of the potential risks and helping them to understand what they can do to keep themselves safe is essential for their well-being. Having regular conversations, understanding what they are using the internet for and assuring them there is a trusted adult they can talk to if anything upsets them online, will help to keep them safe.

Those working with children, young people and adults at risk are expected to support them to develop the skills they need to use the internet and social media safely for learning and enjoyment. Employees and carers must keep children and young people in their care as safe in the online world as in the real world.

3.1 Responsibilities

Online safety is important in all the Group's settings and agencies. Different services, and employees within them, may have different roles in keeping children, young people and adults safe online but it must always be treated as a high priority.

3.1.1 Fostering

Foster carers play a vital role in helping to keep children and young people in their care safe; dealing with their vulnerabilities online is as important as in the real world.

The Group has produced a comprehensive guide for foster carers to help identify risks and support the children and young people they care for to stay safe online:
https://www.nfa.co.uk/story/story_category/keeping-children-safe-online-a-foster-carers-guide-to-internet-safety/

3.1.2 Residential Settings

Those caring for and supporting children and adults in residential settings play a vital role in helping to keep them safe in the offline and online worlds.

The UK Safer Internet Centre provides advice, information and links to toolkits to help keep those in residential settings safe online. Please go to the following websites to access these resources:

https://www.saferinternet.org.uk/advice-centre/residential-care-settings
https://www.saferinternet.org.uk/blog/supporting-vulnerable-groups-online

3.1.3 Schools

Digital technology, the internet and related applications provide a wealth of fabulous learning opportunities and have many positive uses in schools. Their use must be balanced with educating pupils about the risks and helping them to take a responsible and safe approach. The school must help and support its children and young people to recognise and avoid online safety risks and to help build their digital resilience.

Childnet provides a range of resources to support online safety in schools:
https://www.childnet.com/teachers-and-professionals

Online safety should be covered in detail as part of the PSHE (Personal, Social, Health & Economic)/ PSE (Personal and Social Education) curriculum in schools.

The Group also requires safe and secure systems to be put in place within schools. An up-to-date Web Filtering Policy template is sent to each school annually, which they are asked to implement in their setting.

4.0 Guidance

The rapid rate of technological development and change can leave many adults overwhelmed and not sure where to start. However, online safety does not require high levels of technical expertise, it requires awareness of the potential risks and an understanding of the steps that can be taken to help keep the children, young people and adults we support safe.

There are many excellent resources available to help, which this guidance provides signposting to. The Group also provides training and support for employees and carers on this subject. Please visit Shine for the latest training available.

4.1 Understanding the Risks

Many of the main risks are highlighted below. However, technology and its risks, advances rapidly. There are many websites that can be accessed to maintain awareness and keep in touch with the latest developments. Some are referenced within the guidance and a list is included in the Helpful Resources section below.

The potential risks from internet use can be classified under the following headings:

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

4.1.1 Harmful Content and Online Groups

Harmful content is anything that causes distress to the person viewing it. Sometimes when using the internet people unintentionally come across content that is harmful or upsetting. False information and fake news can also be a cause of distress.

There are many positive groups and forums online that can be very helpful. However, there are also groups that promote harmful behaviours such, as anorexia, suicide, self-harm and substance

abuse. It is important to be aware of what the children, young people and adults we support are doing online and what they are talking about.

The dark web is more difficult to access but is something to be aware of, particularly for those with a keen interest and expertise in computing. It is a section of the internet used for illegal transactions, such as guns, drugs, human trafficking or accessing images of child sexual abuse. For further information, https://www.thinkuknow.co.uk/parents/articles/what-is-the-dark-web/

For information about reporting harmful content, please go to: https://reportharmfulcontent.com/

4.1.2 Cyberbullying

Cyberbullying is bullying using digital technologies. It can take place through social media, messaging, gaming and mobile phones. It is repeated behaviour, aimed at scaring, upsetting or shaming those who are targeted. The bullying can continue when the young person is at home through their digital devices.

The National Bullying helpline has produced a guide for different apps giving detailed the steps on how to block or report a bully via some of the most popular social platforms: https://www.nationalbullyinghelpline.co.uk/social-media.html

4.1.3 Sharing images and information

The children, young people and adults we support need to develop an understanding of the potential consequences and permanency of the information they share online. Once information is online it is hard to remove and can be copied and shared. This can provide other people with information about their identity, location and personal interests.

Photographs of individuals in the Group's care must not be posted online or on social media by employees or carers. Children should be strongly discouraged from doing this as they could place themselves at risk of harm or jeopardise the security of their placement. If photographs need to be sent by email, this should be done securely. Personal emailing of photographs of those we support is not allowed.

Please see the Images of Children Policy for further information for carers.

4.1.4 Sexting

Sexting describes the sending and receiving of sexually explicit or provocative images via text, email, messaging or on social networking sites.

This can lead to negative comments, bullying and make the individual more vulnerable to exploitation and blackmail. Images can spread quickly over the internet and through social media, which can affect the persons reputation and cause emotional distress. It could also affect their lives in the future, e.g. when applying for a job.

Creating an image of a person under the age of 18 is illegal, even if they take it and send it themselves.

4.1.5 Grooming

Grooming is when someone develops an emotional connection with an individual to gain their trust for the purposes of abuse, exploitation, radicalisation or trafficking. This can happen online or face-to-face. The online world makes it easier for people to remain anonymous and create an image of themselves that may not be true.

4.1.6 Smartphone Apps and Gaming

Smartphone apps are gradually taking over traditional web browsing and online gaming, with thousands available to download. Most are safe to use, however, some carry age restrictions or are unsuitable for youngsters. Apps can be easily exploited by online criminals, who can contact children, young people and adults at risk through the interface or access their personal information and data, including their location.

It is important to be aware of the apps the people in our care are downloading to their phone or tablet; its suitability needs to be checked to make sure they are not unwittingly sharing private data with cybercriminals or doing something that will cause them distress.

Foster carers and employees in residential settings should ensure that children and adults who enjoy gaming activities, do so in healthy way. Gaming can be addictive. Excessive gaming can contribute to a sedentary lifestyle and have an adverse impact on emotional and physical health. Appropriate boundaries in this regard should be outlined in care planning and risk assessment documentation.

Employees in schools that have concerns about the effect of gaming on children's health and wellbeing should report this to a Designated Safeguarding Lead (DSL).

4.1.7 Child Sexual Exploitation (CSE)

CSE is a type of sexual abuse and happens in both the offline and online world. When this happens online, young people may be persuaded or forced to:

- Send or post sexually explicit images of themselves.
- Take part in sexual activities via a webcam or smartphone.
- Have sexual conversations by text or online.
- Abusers may threaten to send images, video or copies of conversations to the young person's friends and family unless they take part in other sexual activity.
- Images or videos may continue to be shared long after the abuse has stopped.

The number of children and young people affected by abuse online is unknown as those subjected to it do not often tell people because they feel ashamed or guilty, they may not know who to tell, or not realise they are being abused.

Please read the Group's Child Sexual Exploitation Policy. If you believe a child is being sexually exploited or at risk of exploitation, please follow the reporting procedures outlined in this policy. Where indecent images of children or other unsuitable material are found, the police and Local Authority Designated Officer (LADO)* or Local Authority/Health and Social Care Trust (as appropriate), must be informed immediately.

*The term LADO applies in England. Scotland and Wales must notify the Local Authority, Northern Ireland must notify the Health and Social Care Trust.

It is important to remember that the law allows for disclosure of confidential information necessary to safeguard a child if there are reasons to believe that a child is experiencing or at risk of suffering significant harm.

CEOP is the Child Exploitation and Online Protection Command and their website thinkuknow has a range of helpful resources, including tools and activities for children of different age groups, a Children's Workforce section and a parent/carer section.

4.1.8 Online Scams (Phishing, SMishing, Vishing)

Scammers target people through mobile phones via text, email or through a phone call. They are usually trying to obtain personal details to enable them to steal money. Being aware of the various methods they use to try and trick people into giving them information will help reduce the risk of becoming a victim of a scam. Some of the common ways they try to extract information are:

- Phishing - when a scam is sent via email, usually asking you to click on a link.
- SMishing - when a scammer sends a message to text.
- Vishing - a voice call scam over a phone.

For further information and advice please go to: Safe Search kids

It is also important to discuss the risks of buying goods online and checking websites are genuine and secure to help prevent young people being scammed or inadvertently buying counterfeit goods.

4.1.9 Additional risks for looked after children

There can be additional risks for looked after children that carers need to be aware of and be equipped to deal with. These can include:

- Unregulated contact from birth family members - contact arrangements must be in line with the agreement that has been made as part of the child's care plan. If contact is not allowed offline, the same applies online.
- Bullying - children in care are sometimes seen as, or feel, 'different' to their peers, and this may place them at an added risk of both bullying and cyberbullying.

5.0 How to help children, young people and adults we support stay safe

5.1 Managing Access

For the children, young people and adults we support, access to the internet and digital devices will be subject to the care planning and review process and will be risk assessed, in agreement with the local authority and family (where appropriate), to help keep them safe in the online world.

Children and young people in foster care should have a Digital Use Agreement in place, setting out what they agree to do to keep themselves safe. Digital risks must also be considered as part of the care planning process, which can be documented within the overall risk assessment or a specific digital risk assessment can be carried out. The following documents are available, or agency templates can be used:

- Young person's digital use agreement
- Digital risk assessment
- Digital family agreement
- Digital Policies Checklist

An E-safety agreement should also be completed for each person supported in residential care.

Acorn Digital Learning has developed a number of useful documents, including a risk assessment and Online/Remote Learning Policy that schools may find helpful to adapt for their settings. Please email: AcornDigitalLearning@nfa.co.uk for further information.

5.2 Setting Boundaries

Setting boundaries helps the children and adults we support to know what is acceptable and help them to feel safe and stay safe. This could include planning what time of day online activity is allowed and how long for, having rules in place such as, no devices after bedtime and only using devices in communal areas.

Remind children, young people and adults we support that no matter how many times they have been in contact with someone online, if they do not know them in the real world, they are stranger, they may not be who they say they are. It is not safe to give them personal details or arrange to meet them.

5.3 Communication and Involvement

Talking to children and those who may be at risk to understand how they are using the internet and social media will help them to stay safe. It is important that they know they can talk to a trusted adult if something concerning happens online, even if it is something they feel embarrassed about.

5.3.1 Starting a conversation about online safety

It can be difficult to know how to start a conversation about online use. The NSPCC and Childnet have provided some helpful suggestions. Please visit their websites:

https://www.nspcc.org.uk/keeping-children-safe/online-safety/talking-child-online-safety/
https://www.childnet.com/parents-and-carers/have-a-conversation

The Group's Digital Family Agreement can also be used to guide a discussion about digital use and behaviour. Some families find it helpful for household members to sign this, others use it as a checklist to guide the conversation.

Emphasising the need to be respectful of other people and only posting and sending friendly messages and content is also important. Children and young people might not realise the impact of comments they make online. It can be helpful to use the THINK acronym before posting anything: is it True, Helpful, Inspiring, Necessary, Kind?

Guidance on what to do if you find out a child in your care is cyberbullying others is available here:
https://www.internetmatters.org/hub/expert-opinion/help-my-child-is-the-cyberbully/

5.4 Security and Privacy Controls

Setting controls on devices is an effective way to reduce risk; they can block or filter upsetting or inappropriate content, and control purchases and activity within apps. Parental control software can be installed on phones, tablets, games consoles, laptops and computers. The following websites provide advice on how to do this:
https://www.nspcc.org.uk/keeping-children-safe/online-safety/parental-controls/

https://www.internetmatters.org/parental-controls/ - gives specific advice on all devices and apps, using drop down boxes to select the specific phone, device, social media, app etc.

https://www.net-aware.org.uk/ - provided by the NSPCC, in partnership with O2, is a guide to the apps, games and social media sites in use, it includes information on age restrictions and gives safety ratings.

Most devices and apps have 'geo-location' options. If this is enabled, it could be sharing the user's location with strangers. This can usually be disabled easily in the device settings.

Where there is an option to do so, apply the "Friends only" setting; people set as 'Friends' should be people they know or trust in the real world. Some apps let people tag others in images and comments, which can result in children being unwittingly tagged into offensive online content. Check tagging settings in social accounts to make sure they cannot be identified by others after being tagged.

Keep apps and devices up to date. If the manufacturer provides an update, they should be installed as soon as possible, as they often include better security provision or offer enhanced protection against malware.

Children and young people are often more tech savvy than most adults, so it is important to keep talking to them and regularly check what apps and social media they are using and the privacy controls. They may know how to alter privacy controls and settings, so it is important to maintain an awareness of their online activity.

Passwords are useful tools to help keep digital devices and sensitive information safe. When choosing your password, ensure it is not easily guessable (e.g. avoid using names of family members, pets or references to memorable dates). Ideally a long password, with a combination of upper and lower-case letters, numbers and symbols should be chosen. Usernames and passwords should not be written down.

6.0 Responding and Reporting

If you have reason to believe that a child, young person or adult we support is experiencing harm or is at risk of harm, the reporting process set out in the Safeguarding Policy must be followed immediately.

If carers or employees become aware of an online incident that is a cause for concern, they should:

- Provide reassurance to the child or adult
- Take immediate action to report any criminal offences to the police and social care
- Inform the child or adult's placing authority and family as appropriate
- Review the supervision and support arrangements for the young person/adult accessing the internet.
- Check the privacy and security settings on the person's devices and account.
- Agree what action will be taken to prevent recurrence and reduce risk, the risk assessment should be reviewed and updated. Consideration of educating young people and adults on internet safety matters should be included.

6.1 Foster Carers

Carers must report any such concerns immediately to the Supervising Social Worker and keep a record of what has happened.

6.2 Residential Care

The incident must be reported to the designated manager and recorded on Info Exchange (Adults)/ Clearcare (Children's). The safeguarding box should be ticked which will trigger an email to safeguarding@ofgl.co.uk and will be picked by the Group Safeguarding Lead.

6.3 Schools

Employees in schools must report any such concerns or incidents to their DSL immediately. The Safeguarding Policy can be found on the School's website.

Employees and Carers are advised to always report any concern or worry straight away, rather than waiting to see if the matter develops. If you are unsure about what action to take or need help or advice you should speak to the DSL, your Line Manager or Social Worker, as appropriate.

You can also contact the Group Safeguarding Lead for advice.

External bodies where concerns can be reported to are:

CEOP: www.ceop.gov.uk www.thinkuknow.co.uk
Internet Watch Foundation: www.iwf.org.uk
Action Fraud to report fraud and internet crime: https://www.actionfraud.police.uk/

7.0 Procedures

Online activity and digital use should be monitored and manged through appropriate supervision, risk assessments, as part of the care planning process, and ongoing review.

Fostering can utilise the documents identified in 5.1.

8.0 Helpful Resources

In addition to the websites mentioned in this document, the following links also provide helpful information:

https://www.nspcc.org.uk/keeping-children-safe/online-safety/

https://www.saferinternet.org.uk/advice-centre/parents-and-carers

https://www.childnet.com/parents-and-carers/hot-topics/keeping-young-children-safe-online

A Practical Guide for Parents and Carers whose children use Social Media

https://parentinfo.org/