Outcomes First Group

STAYING SAFE ONLINE

Group Policy

STAYING SAFE ONLINE

CONTENTS

1.0 Purpose 2
2.0 Policy Statement 2
3.0 Legislation & Policy Framework 2
4.0 Supporting children and young people 4
5.0 Guidance 4
6.0 Understanding the Risks 5
7.0 How to help children and young people stay safe 8
8.0 Responding and Reporting 9
9.0 Helpful Resources 10

Terminology - please note that the terms "our teams" and "team member/s" include everyone working in Outcomes First Group's services in a paid or unpaid capacity, including employees, consultants, agency staff and contractors.

1.0 Purpose

We are committed to ensuring that all the children and young people we educate and support are safeguarded at all times, both offline and online. Their safety is our highest priority and must remain central to everything we do. This document sets out our policy for online safety and provides guidance to help keep the children and young people we educate and support safe online and when using digital devices.

2.0 Policy Statement

Technology is part of everyday life and provides many possibilities, including tools for learning, socialising, playing and helping people find their place in the world. However, it also carries significant risks to which some of the children and young people we educate and support can be more susceptible to 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 doing online and using digital technology 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 and young people are expected to support them to develop the skills they need to use the internet, social media and digital devices safely for learning and enjoyment. Team members must strive to keep our children and young people as safe in the online world as in the physical world.

3.0 Legislation & Policy Framework

Across the UK, criminal and civil legislation aims to prevent abusive activities online including: stalking and harassment; improper use of any public communications; sending indecent, offensive; false or threatening communications; and sending private sexual photos or videos of another person without their consent.

The UK Online Safety Act 2023 aims to minimise the risks of online harm to users, especially children, by putting duties on providers of online services to make them legally responsible for keeping people, especially children, safe online. Ofcom has published Protection of Children from Online Harm Codes and Guidance in 2025. For further information about how the legal duties are being implemented, please see: Ofcom - Online Safety

The legislation and subsequent codes and guidance are a positive step forward; however, it is important that team members maintain vigilance in helping those we support to stay safe online.

For further information about the legal framework and related information, please see the NSPCC's Preventing online harm and abuse

Governments of the UK nations have developed further guidance and plans to help keep children and young people safe from online harm and abuse:

- Advice on keeping children safe from abuse and harm UK Government
- Teaching online safety in schools DFE Guidance
- Enhancing digital resilience in Education: An action plan Welsh Government
- Safeguarding Children from Online Abuse Welsh Government
- Internet Safety for children and young people: National Action Plan – Scottish Government
- Preventing and tackling bullying and Cyber-bullying: advice for schools
- Relationships and sex education
- Searching, screening and confiscation
- Generative AI Product Safety Expectations

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

- Safeguarding Policy
- Anti-Bullying Policy and Guidance
- Child-on-child Abuse Policy/ Peer-on-peer abuse Policy
- Behaviour Policy (Person-centered and neurodivergence-affirming)
- Gaming Devices Best Practice Guidance
- Child Exploitation Policy and Guidance
- Protecting Children & Young People against Radicalisation Policy
- Photography of Injuries and Medical Conditions Policy
- Web-Filtering and Monitoring Policy
- Mobile and Smart Technology Policy
- AI Policy and AI Acceptable Use Policy
- Code of Conduct & Ethics
- Parent/Carer-School Communications Policy, and
- the Group's Safeguarding Statement and policies on Personal Device Use, Mobile Devices, Password Protection, Information Security, Data Protection and GDPR

For those we support who are non-verbal or have limited receptive and expressive communication and learning disabilities, more direct on-going observation of their technological use to support them is required to keep them safe, along with direct modelling of safe online behaviour by those responsible for their care and education.

The Group operates a highly secure web filtering system on the internet link to the setting which safeguards the setting's computers and internet use, and it also offers safeguards on mobile phones and tablets used over the setting's Wi-Fi network. Web filtering and monitoring helps to keep young people safe from illegal content and protect them from extremism online when using the setting's Wi-Fi, it is informed in part, by the risk assessment required by the Prevent Duty. Please note that the web-filtering system is not able to apply protection when devices are used outside of the Group's sites or when using Mobile Data Networks. Please see the *Web-Filtering and Monitoring Policy* for further information.

4.0 Supporting children and young people

Digital technology, the internet and related applications provide a wealth of fabulous learning opportunities and have many positive uses in schools and colleges. Their use must be balanced with educating pupils and students about the risks and helping them to take a responsible and safe approach.

Schools and colleges must help and support their pupils and students to recognise and avoid online safety risks and to develop their digital resilience. Pupils and students that have limited receptive and expressive communication and learning disabilities will require more direct on-going observation of their technological use to keep them safe.

Childnet provides a range of Help, advice and resources for teachers and professionals

DFE has published guidance for schools and colleges on Harmful online challenges and online hoaxes, which includes advice on responding appropriately to incidents involving harmful online challenges and online hoaxes, preparing for future online challenges and hoaxes, sharing information with parents and carers and where to get help and support.

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

Schools and colleges are expected to meet the DFE's Filtering and monitoring standards for schools and colleges Please also see the *Web filtering and Monitoring Policy* for further details.

The school/college will carry out an annual review of their approach to online safety, supported by an annual risk assessment that considers and reflects the risks children and young people face. Free online safety self-review tools for schools can be found at https://360safe.org.uk/

Each school/college also has a *Mobile and Smart Technology Policy*. Information about standards schools and colleges should meet on cyber security, user accounts and data protection can be found here: Cyber security standards for schools and colleges

Schools and colleges are encouraged to use the regular communications they have with parents and carers to reinforce the importance of children and young people being safe online and keep them informed about what systems the school/ college uses to filter and monitor online use, what their child is being asked to do online at school or college, including the sites they will be asked to access, and be clear who from the school or college (if anyone) their child is going to be interacting with online.

DFE has published Generative AI Product Safety Expectations to support schools and colleges to use generative artificial intelligence safely, and explains how filtering and monitoring requirements apply to the use of generative AI in education.

5.0 Guidance

The rapid rate of technological development and change can leave many adults overwhelmed. 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 and young people safe.

In addition to the resources available signposted in this document, please also visit Shine, our Learning Management System, for the latest training available.

6.0 Understanding the Risks

Many of the main risks are highlighted below. However, technology and its risks advance 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 further links are included in Section 9.0.

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

- Content: being exposed to illegal, inappropriate or harmful material for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- Contact: being subjected to harmful online interaction with other users
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm
- Commerce: risks such as online gambling, inappropriate advertising, phishing and/or financial scams. (Please report phishing emails to the Anti-Phishing Working Group (https://apwg.org/)

6.1 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, substance abuse and radicalisation. It is important to be aware of what our children and young people 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. Please also see: What is the dark web?

For information about reporting harmful content, please go to: Report harmful content

6.2 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 child/young person is at home through their digital devices.

Please also see National Bullying Helpline - Social Media for a guide to different apps, with detailed steps on how to block or report a bully via some of the most popular social platforms.

Internetmatters provide advice on what to do if a child we support is cyberbullying others.

6.3 Sharing images and information

The children and young people we support need to be aware of the potential consequences and permanence 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. Children and young people should be strongly discouraged from doing this as they could place themselves at risk of harm.

Photographs of children and young people the school/college the educates and supports must not be posted online or on social media by team members. If photographs need to be sent by email, this should be done securely. Personal emailing of photographs of those we educate and support is not allowed.

Team members should also be aware of the Photography of Injuries and Medical Conditions Policy and CCTV Policy.

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 and bullying that can make the individual more vulnerable to exploitation and blackmail.

Images can spread quickly over the internet and through social media, which can affect the person's reputation and cause emotional distress. It could also affect their lives in the future, e.g., when applying for a job.

Taking, making, sharing and possessing indecent images and pseudo-photographs of people under 18 is illegal. A pseudo-photograph is an image made by computer-graphics or otherwise which appears to be a photograph. This can include photos, videos, tracings and derivatives of a photograph and data that can be converted into a photograph.

6.4 Grooming

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

6.5 Smartphone Apps and Gaming

Smartphone apps are very popular and there are 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 and young people 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.

Team members in residential settings should ensure that children and young people who enjoy gaming activities do so in a 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.

Any concerns about the effect of gaming on children's mental health and wellbeing should be reported to the DSL. Please also see the Group's *Gaming Devices Best Practice Guidance*.

6.6 Child Exploitation

Please also see the Child Exploitation Policy

Child Sexual Exploitation (CSE) and Child Criminal Exploitation (CCE) are forms of abuse that occur where an individual or group takes advantage of an imbalance in power to coerce, manipulate or deceive a child into taking part in sexual or criminal activity. This happens both offline and online.

Online Grooming describes the process of developing a friendship or relationship with a child online, with the intention of abusing or exploiting them, and can include sexual or criminal exploitation as well as extremism. Offenders may use social networks, online games or live streaming sites to identify and communicate with young people.

Online abuse and exploitation can:

- Occur through online chats, pictures, videos or webcams and the young person may never physically meet their abuser
- Begin online then move offline
- Be perpetrated by individuals or groups, males or females, other children or adults
- Be a one-off or a series of incidents over time.

In cases of online sexual exploitation, 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 as they feel ashamed or guilty, they may not know who to tell, or may not realise they are being abused.

Please read the *Child 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 or equivalent must be informed immediately.

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.

The Child Exploitation and Online Protection Command (CEOP) website has a range of helpful resources, including tools and activities for children of different ages, a section for professionals working with children and young people, and a parent/carer section.

6.7 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 children and young people being scammed or inadvertently buying counterfeit goods.

6.8 Additional risks for looked after children

There can be additional risks for looked after children that team members 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 any 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.

7.0 How to help children and young people stay safe

7.1 Managing Access

As part of the induction into our schools, all pupils and students and parents/carers/ those with parental responsibility are required to sign an IT user agreement/ E-safety agreement.

For children and young people with an EHCP in our schools and colleges and all those in residential settings, the child/young person's IT User-agreement/ E-Safety agreement will be completed in line with their care plan, and access to the internet and digital devices will be subject to care planning and review process and will be risk assessed. This will be done in agreement with the local authority and family (where appropriate), to help keep them safe in the online world.

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@ofgl.uk for further information.

7.2 Setting Boundaries

Setting appropriate boundaries helps the children and young people we support to know what is acceptable and help them to feel safe and stay safe. For those in residential homes, boundaries regarding 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 will need to be considered.

Our children and young people should be regularly reminded 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 strangers, and they may not be who they say they are. It is not safe to give them personal details or arrange to meet them.

7.3 Maintaining professional boundaries

Please also see the Group's Code of Conduct & Ethics Policy.

Team members must maintain professional boundaries both inside and outside of working hours with children and young people who are currently, and have previously, attended the Group's services. For example, team members should not accept friend requests from the children and young people they educate or support.

Any on-going contact arrangements with children or young people who have left the Group's services or settings must be managed professionally and sensitively and in a way that protects the child/young person and the team member.

7.4 Communication and Involvement

Communicating with children and young people, 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 or notify a trusted adult if something concerning happens online, even if it is something they feel embarrassed about.

For those who are non-verbal or have limited receptive and expressive communication, arrangements for direct observation of their technological use is required to keep them safe. This should be written in their care plan and risk assessment and must be specific to their individual needs to mitigate the risks, it should not be a blanket approach of restriction. Direct modelling of safe online behaviour by those providing care and education is also important.

7.5 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.

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?"

7.6 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: NSPCC - Parental-controls, Internet Matters - Parental Controls and Digital Parenting Pro give helpful information and advice about available parental controls and safety settings across devices and popular apps, games and social media.

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, the "Friends only" setting should be applied; 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 and young people 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.

Apps and devices should be kept 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 communicating with them about this 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.

8.0 Responding and Reporting

If you have reason to believe that a child or young person 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 a team member becomes aware of an online incident that is a cause for concern, they should:

- Provide reassurance to the child/young person
- Take immediate action to report any criminal offences to the police and social care
- Inform the child/young person's placing authority and family as appropriate
- Review the supervision and support arrangements for the young person 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 further educating children and young people on internet safety matters should be included.

In schools and colleges – team members report any such concerns or incidents to their DSL immediately. The incident must also be recorded on the Electronic Recording System and an email sent to safeguarding@ofgl.co.uk to notify the Director of Safeguarding/ Safeguarding Adviser. Please also see the Safeguarding Policy.

In residential care - The concern or incident must be reported to the Safeguarding lead/Registered Manager and recorded on Home's Electronic Recording System and an email sent to safeguarding@ofgl.co.uk to notify the Director of Safeguarding/ Safeguarding Adviser. Please also see the setting's Safeguarding Policy.

Team members 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/Safeguarding Lead, your Line Manager or the Headteacher, Principal or equivalent, as appropriate. Team members can also contact the Director of Safeguarding/Safeguarding Adviser for advice.

External bodies where concerns can be reported are:

CEOP Education

Internet Watch Foundation (IWF)

Action Fraud - to report fraud and internet crimes

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

For the children and young people we support in residential care that require direct monitoring and intervention, this must be clearly written into their care plan and risk assessment, explaining how this meets their individual needs to help keep them safe online.

9.0 Helpful Resources

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

NSPCC Keeping Children Safe Online Safety

NSPCC Online Safety Families Children with Send

Social Media Guidance for parents and carers

Cerebra - Learning Disabilities, Autism and Internet Safety

UKCIS (UK Council for Internet Safety)

Star Send toolkit

Ambitious about Autism - Online safety information

Stop It Now! (UK and Ireland)

Child Protection Scotland - Online Abuse

Swgfl.org.uk Artificial Intelligence and Swgfl.org.uk Synthetic media (Deepfakes)

Outcomes
First Group