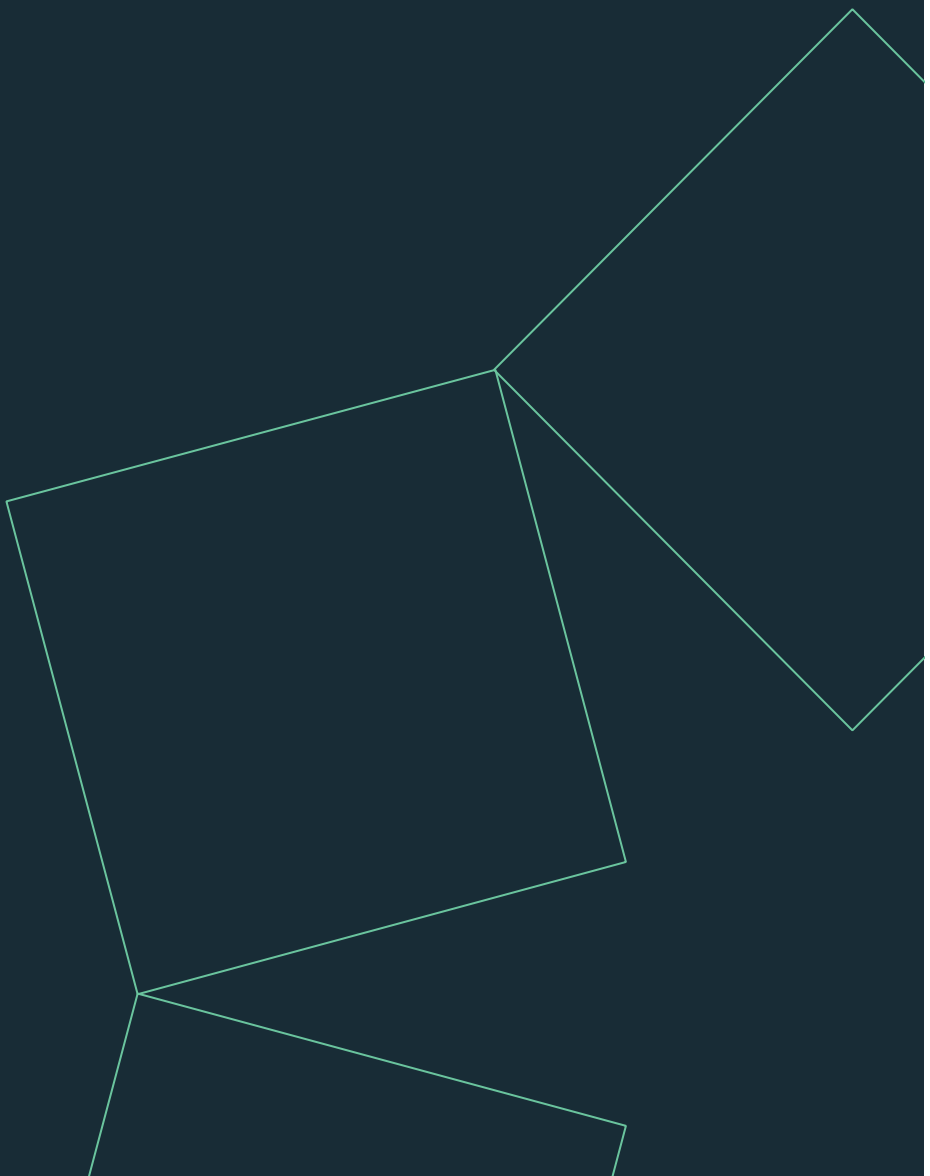
OFG Education

STAYING SAFE ONLINE

Group Policy



OFG Education

STAYING SAFE ONLINE

CONTENTS

1.0 Purpose 3
2.0 Policy Statement 3
3.0 Legislation & Policy Framework 3
4.0 Roles and Responsibilities 4
5.0 Whole-setting to Online Safety 4
5.1 Online Safety Education and digital resilience 5
5.2 Web Filtering and Monitoring 5
5.3 Team Member Awareness and training 6
5.4 Working with Parents and Carers 6
5.5 Additional and individualised Support 6
6.0 Understanding the Risk 6
6.1 Content Risks 7
6.2 Contact Risks 8
6.3 Conduct Risk 9
6.4 Commerce risks 10
6.5 Other technology-specific considerations 11
6.6 Students who may be at increased risk 11
7.0 Helping students to stay safe 12
7.1 Communication and Involvement 12
7.2 Managing Access 12
7.3 Security and Privacy Controls 12
7.4 Maintaining professional boundaries 12
8.0 Responding and Reporting 12
9.0 Digital Wellbeing 13
10.0 Helpful Resources 13

Terminology

- "Our teams" and" "team member/s" include everyone working in Outcomes First Group's settings and services in a paid or unpaid capacity, including employees, consultants, agency staff, trainees and contractors. For Blenheim schools, volunteers are included in this definition.
- "Parents and carers" refer to the person or -people with legal parental responsibility for the child/young person
- "Students" refers to all children and young people being educated and supported at the setting or service

1.0 Purpose

We are committed to ensuring that our students are safeguarded both offline and online. Their safety is our highest priority and is central to everything we do. This document sets out our policy for online safety and provides guidance to help keep our students safe online and when using digital devices.

2.0 Policy Statement

Technology is an integral part of modern life and offers significant opportunities for learning, communication, creativity, entertainment and participation in society. Digital technologies can support educational achievement, social connection and personal development. However, they can also expose children and young people to a range of risks and harms, some of which may have a significant impact on their safety, wellbeing and development.

Online risks continue to evolve rapidly and may include exposure to inappropriate content, online abuse, cyberbullying, grooming, exploitation, artificial intelligence (AI) generated content, deepfakes, harmful online challenges, misogyny, extremist content, disinformation, financial exploitation, scams, image-based abuse and the misuse of live-streaming platforms. Students who are vulnerable, have Special Educational Needs and Disabilities (SEND), or who are already experiencing harm or risk offline may be at increased risk online. The school/college therefore maintains a proactive approach to identifying, assessing and responding to emerging online risks.

Promoting online safety and digital resilience is a key aspect of our safeguarding responsibilities. We recognise the importance of helping students understand the benefits and risks of technology, develop safe online behaviours, recognise potential concerns and know how to seek help when needed. Regular conversations about online activity, alongside strong relationships with trusted adults, play an important role in helping children and young people stay safe.

We are committed to providing an environment where students can learn, communicate and use technology safely and responsibly. Through education, support, monitoring and appropriate safeguards, team members help students develop the knowledge, skills and confidence needed to use the internet, social media, online services and digital devices safely for learning, enjoyment and participation in the wider world.

3.0 Legislation & Policy Framework

This policy has been developed in line with relevant legislation, statutory guidance and recognised best practice, including:

UK-wide Legislation and regulation

- Online Safety Act 2023
- UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018
- Protection of Children from Online Harm Codes and Guidance (Ofcom)

England

- Keeping Children Safe in Education (KCSiE) (England)
- Working Together to Safeguard Children (England)
- Teaching online safety in schools (DFE Guidance)
- Relationships and sex education (RSE) and health education (DFE Guidance)
- Searching, screening and confiscation (DFE Guidance)
- Prevent Duty Guidance

Wales

- Keeping Learners Safe
- Enhancing digital resilience in Education: An action plan
- Safeguarding Children from Online Abuse

Scotland

- National Guidance Child Protection (Scotland)
- Internet Safety for children and young people: National Action Plan (Scotland)
- Generative AI Product Safety Expectations (DFE Guidance)

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

- Safeguarding Policy
- Web-Filtering and Monitoring Policy
- Mobile and Smart Technology Policy
- Anti-Bullying Policy and Guidance
- Child-on-child Abuse Policy/ Peer-on-peer abuse Policy
- Behaviour Policy
- Gaming Devices Best Practice Guidance
- Child Exploitation Policy and Guidance
- Protecting Children & Young People against Radicalisation Policy
- Use of Images Policy
- AI Policy and AI Acceptable Use Policy
- RSHE 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

4.0 Roles and Responsibilities

All team members who work directly or indirectly with students in our schools and colleges have a responsibility to safeguard their welfare, both offline and online. The following have specific responsibilities:

- The Headteacher/Principal is responsible for ensuring effective implementation of this policy within their setting.
- The DSL is responsible for oversight of online safeguarding concerns, trends and reporting.
- IT Services are responsible for maintaining filtering, monitoring and cyber security arrangements.
- The Safeguarding & Quality (S&Q) Committee receives assurance regarding online safety arrangements through safeguarding reporting.

5.0 Whole-setting to Online Safety

All online safety concerns must be reported immediately to the Designated Safeguarding Lead (DSL) and managed in accordance with Safeguarding Policy.

5.1 Online Safety Education and digital resilience

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 students about the risks and helping them to take a responsible and safe approach.

The rapid pace of developing digital technologies, online services and AI can leave professionals and parents/carers feeling less confident in navigating an increasingly complex online landscape. However, effective online safety does not depend on advanced technical knowledge, it requires an awareness of potential risks, an understanding of how children and young people are engaging with technology, and a willingness to take practical steps to promote safe, responsible and positive online communication.

The school/college supports students to recognise and avoid online safety risks and to develop their digital resilience. Online safety is covered in detail as part of the PSHE (Personal, Social, Health & Economic) curriculum in schools. Students who have limited receptive and expressive communication and learning disabilities will require more direct on-going observation of their technological use to keep them safe.

Our *Mobile and Smart Technology Policy sets out* our approach to the use of such devices by students, team members, parents/carer and visitors in the setting. Personal electronic devices, including phones, smart watches and iPads, brought onto site by students must be handed in at the school/college reception, and are only allowed in exceptional circumstances, under specific agreements. Please see the Policy for further details.

5.2 Web Filtering and Monitoring

We are committed to meeting the DFE's Digital and technology standards, including the Cyber Security Standards for Schools and Colleges.

Secure filtering and monitoring systems are in place to help safeguard students from illegal, inappropriate and harmful online content. These arrangements support the prevention of online abuse, exploitation, radicalisation and other safeguarding risks and are informed by the risk assessment required by the Prevent Duty.

Filtering and monitoring alerts that identify safeguarding concerns must be reviewed promptly and form part of the school's wider safeguarding arrangements.

Filtering and monitoring systems apply to devices connected to the school's/college's network and Wi-Fi services and when using the Group's devices outside of a Group site.

The Headteacher/Principal, Designated Safeguarding Lead (DSL) and IT Services work together to ensure that filtering and monitoring arrangements remain effective, proportionate and responsive to emerging risks. Any weaknesses, breaches or concerns relating to web filtering or monitoring systems must be reported immediately to the DSL and IT Services and reviewed promptly to ensure students remain appropriately safeguarded.

The effectiveness of the school's/college's online safety arrangements, including filtering and monitoring systems, is reviewed at least annually and whenever significant safeguarding concerns arise. Reviews are informed by a risk assessment of current and emerging online risks and may be supported by recognised self-review tools, such as the 360 Safe Online Safety Self-Review Tool

Further information is available in the *Web Filtering and Monitoring Policy*.

5.3 Team Member Awareness and training

All team members must complete the Group's mandatory *Online Safety and Cyberbullying* training and other relevant training required for their role. Team members are expected to maintain awareness of current and emerging online risks, including online abuse, exploitation, cyberbullying, artificial intelligence (AI), deepfake content, harmful online challenges, extremist content, image-based abuse, misinformation and scams.

The DSL and senior leaders will ensure regular updates on online safety and emerging risks are provided. Team members must ensure they understand how to identify, respond to and report online safety concerns in line with the *Safeguarding Policy.*

A range of helpful resources are available, including:

- Childnet provides guidance, training materials and practical resources for teachers and other professionals working with children and young people.
- Guidance on Harmful online challenges and online hoaxes, which includes advice on prevention, safeguarding children and young people, working with parents and carers, and accessing appropriate support.

5.4 Working with Parents and Carers

The school/college uses our regular communications with parents and carers to reinforce the importance of online safety 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/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.

5.5 Additional and individualised Support

For students who are non-verbal or have limited receptive and expressive communication and learning disabilities, 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.

For children in the Early Years Foundation Stage (EYFS), online safety education will be delivered in an age-appropriate manner through supervised use of technology, direct teaching, stories, play-based learning and discussions that help develop an understanding of safe and respectful behaviour when using digital devices.

6.0 Understanding the Risk

Many of the main online risks are outlined below. However, as digital technologies, online services and associated risks continue to evolve rapidly, there are a range of reputable websites can be used to maintain awareness about emerging risks and effective safeguarding measures. Some are referenced within this section 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 or generative AI applications that simulate this; 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.
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm for example, making, sending and receiving explicit images, including those generated using AI and online bullying, and
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and/or financial scams. (If you feel students or team members are at risk, in addition to reporting to the DSL, please report to the Anti-Phishing Working Group

6.1 Content Risks

6.1.1 Harmful and Distressing Content

Harmful content is anything that causes distress to the person viewing it. Sometimes users may 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 students are doing online and what they are talking about.

Students may encounter online content that promotes misogyny, male supremacy, violence against women and girls, harmful relationship norms or coercive and controlling behaviour. Exposure to this content may have a significant impact on beliefs, attitudes and behaviour and should be regarded as an online safeguarding concern.

The dark web is more difficult to access but is something to be aware of, particularly with students who have a keen interest and expertise in technology. It is a concealed part of the internet that requires specialised software to access. Although it has some legitimate uses, it is frequently associated with illegal activity and harmful content, including child sexual abuse material. While most students are unlikely to access the dark web, team members should remain aware of the associated and be vigilant to signs that a students may be attempting to access such environments. For further information, please see: What is the dark web?

In addition to reporting in line with the *Safeguarding Policy*, harmful content can be reported at: Report harmful content

6.1.2 Artificial Intelligence and Generative AI

Artificial intelligence (AI) and generative AI tools are increasingly accessible to students. Whilst these technologies can support learning and creativity, they also present risks, including:

- Exposure to inaccurate, misleading or harmful information
- AI-generated content that promotes harmful beliefs, self-harm, eating disorders, extremism or unsafe behaviours
- Deepfake images, videos or audio recordings
- Cyberbullying or harassment through AI-generated content
- Sharing personal or sensitive information with AI systems
- Over-reliance on AI for learning or decision-making

Students should be supported to critically evaluate information generated through AI systems and understand that AI responses may not always be accurate, appropriate or safe.

Guidance on Generative AI Product Safety Expectations has been published by DfE to support the safe use of generative artificial intelligence in education settings.

6.2 Contact Risks

6.2.1 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.

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.

6.2.2 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 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.

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

6.2.3 Live streaming

Live streaming platforms may expose children and young people to grooming, exploitation, inappropriate content and unsolicited contact from strangers. Students should understand that information shared during live streams may be recorded, copied and distributed without their consent.

6.2.4 Online Relationships and Contact with Strangers

Students 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.

6.3 Conduct Risk

6.3.1 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.

The National Bullying Helpline provides a guide to different apps, with detailed steps on how to block or report a bully via some of the most popular social platforms.

Please also see the *Anti-bullying Behaviour Policy*

6.3.2 Sharing images, information and digital footprints

Our students 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. Students should be strongly discouraged from doing this as they could place themselves at risk of harm.

Advances in AI have made it easier to create realistic but false images, videos and audio recordings, often referred to as "deepfakes" or “synthetic media”. These may be used to harass, blackmail, bully, exploit or manipulate children and young people. Any concerns relating to the creation, possession or sharing of deepfake content involving students must be treated as a safeguarding concern and reported to the DSL immediately.

Students should be supported to understand that their online activity contributes to a permanent digital footprint which may affect future education, employment and personal opportunities.

Photographs and videos of students must not be posted online or on social media by team members. If photographs or videos need to be sent by email, this should be done securely. Personal emailing of photographs of students is not allowed.

Please also see the *Use of Images* Policy and *CCTV* Policy.

6.3.3 Online Sexual Harassment

Online sexual harassment can include unwanted sexual comments or messages, pressuring others to share images, sexualised bullying, sharing sexual rumours, creating or sharing sexually explicit content without consent.

6.3.4 Sharing nudes and semi-nudes

The sharing nudes and semi-nudes, including the creation, possession or sharing of nude or semi-nude images, videos or live streams by children and young people, including those that have been generated or altered using AI, can occur via text, email, messaging or on social networking sites.

Images can spread quickly over the internet and through social media, which can affect the person's reputation, cause emotional distress, lead to bullying and make an individual more vulnerable to exploitation and blackmail. 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.

Where indecent images of children or other unsuitable material are found, the police and Local Authority Designated Officer or equivalent must be informed immediately.

6.4 Commerce risks

6.4.1 Online Scams (Phishing, SMishing, Vishing)

Scammers increasingly target children and young people through emails, text messages, social media, online games and phone calls. Their aim is often to obtain personal information, account details or money. Educating students about common scams can help reduce the risk of exploitation and financial harm.

Common types of scams include:

- Phishing – fraudulent emails designed to encourage recipients to click on links, open attachments or share personal information.
- Smishing – scam messages sent via SMS or messaging apps.
- Vishing – fraud carried out through phone or voice calls.

Older students and college learners may be particularly vulnerable to more sophisticated scams, including:

- Cryptocurrency and investment scams
- In-game fraud and account theft
- Romance and relationship scams
- Money mule recruitment, where young people are persuaded to move or receive money on behalf of criminals

The school/college will provide age-appropriate education on recognising scams, protecting personal information and verifying that websites and sellers are genuine and secure. UKSIC provides helpful resources for 11-19s

6.5 Other technology-specific considerations

6.5.1 Mobile 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 younger children. 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.

6.5.2 Gaming can provide opportunities for enjoyment, learning and social interaction. However, excessive or inappropriate gaming may negatively affect a student's wellbeing, physical health, sleep, attendance, relationships or educational progress. Schools should promote safe and balanced gaming habits and work with parents/carers where concerns arise. Any concerns about the impact of gaming on a student's welfare or safeguarding should be reported to the DSL. Further information is available in the Group's *Gaming Devices Best Practice Guidance*.

6.5.3 Emerging Technologies

Emerging technologies, including AI, virtual reality, augmented reality, immersive online environments, AI-powered chatbots and future digital platforms, may expose students to inappropriate content, misinformation, manipulation, exploitation, privacy risks or harmful online interactions. The school/college will remain alert to emerging technologies and trends, ensure online safety education remains current, and support students to develop the critical thinking and digital resilience needed to use new technologies safely, responsibly and effectively.

6.6 Students who may be at increased risk

6.6.1 Looked after children and previously looked after children

Looked after children and previously looked after children may face additional online safety risks. Team members should be aware of these vulnerabilities and provide appropriate support. Risks may include unauthorised online contact from birth family members or others where contact restrictions are in place through care arrangements, as well as an increased risk of bullying or cyberbullying due to children feeling, or being perceived as, different from their peers. Any concerns should be managed in accordance with the child's care plan and reported to the DSL.

6.6.2 Students with Special Educational Needs and Disabilities (SEND)

Students with special educational needs and disabilities (SEND) may face increased online safety risks due to factors such as communication difficulties, social vulnerability, limited understanding of online relationships, or reduced ability to recognise and respond to risk. Online safety education and safeguarding arrangements should therefore be tailored to their individual needs, helping them to develop the knowledge, skills and resilience required to use technology safely while ensuring appropriate levels of support, supervision and protection are in place.

Please see 4.5 for managing online safety for students who are non-verbal or have limited receptive and expressive communication.

6.6.3 Students already experiencing risk or harm offline

Students already experiencing harm, adversity or vulnerability are often at greater risk online. Experiences such as abuse, neglect, exploitation, bullying, social isolation, poor mental health or challenging family circumstances can increase susceptibility to online harms, including grooming, exploitation, cyberbullying, harmful content and coercive or manipulative relationships. It is therefore important that online safety is considered as part of a student's wider safeguarding needs and support arrangements.

7.0 Helping students to stay safe

7.1 Communication and Involvement

Communicating with students 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. The NSPCC and ChildNet provide some helpful suggestions to help with conversations about online use.

Emphasising the need to be respectful of other people and only posting and sending friendly messages and content is also important. Students 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?"

7.2 Managing Access

As part of the induction into our school/college, all students and parents/carers are required to sign an IT user agreement/ E-safety agreement.

For students with an EHCP, their 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.

7.3 Security and Privacy Controls

Students will be supported to understand and use appropriate privacy, security and location settings, protect their personal information, use secure passwords and keep devices and applications updated.

The school/college will provide developmentally appropriate guidance to students and, where relevant, parents and carers about available safety and parental controls.

Further guidance is available through the resources listed in Section 9.0

7.4 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 students who are currently, and have previously, attended the setting. For example, team members should not accept friend requests from the students they have educated or supported.

Any on-going contact arrangements with students who have left the school/college must be managed professionally and sensitively and in a way that protects the child/young person and the team member.

8.0 Responding and Reporting

Any concern that a student is experiencing or is at risk of harm must be reported immediately in accordance with the *Safeguarding Policy*. Team members should:

- support the student
- report the concern to the DSL without delay
- record the incident on the setting's Electronic Recording System
- notify the Director of Safeguarding/Safeguarding Adviser via safeguarding@ofgl.co.uk

Concerns should always be reported promptly rather than waiting for further information or developments. Where advice is needed, team members should consult the DSL, Headteacher/Principal, or Director of Safeguarding/Safeguarding Adviser.

In addition to internal reporting, concerns relating to online safety may also be reported to: CEOP Education; Internet Watch Foundation (IWF); Action Fraud

9.0 Digital Wellbeing

Technology plays an important role in education, communication, and daily life. However excessive, unhealthy, or unbalanced use may affect a student's emotional wellbeing, physical health, sleep, relationships, attendance, engagement, and learning.

The school/college promotes healthy and balanced use of technology and supports students to develop positive digital habits. Students will be encouraged to:

- maintain a healthy balance between online and offline activities
- protect their sleep and wellbeing by establishing appropriate routines around device use
- understand the potential impact of social media, online content and algorithms on emotions, self-esteem, and behaviour
- seek support if online activity is causing distress, anxiety, pressure, or other wellbeing concerns; and
- engage with technology in a safe, positive and purposeful manner.

Team members should remain alert to signs that online activity, gaming, social media, or technology use may be negatively affecting a student's wellbeing and respond appropriately in line with safeguarding and pastoral procedures.

10.0 Helpful Resources

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

UKCIS (UK Council for Internet Safety)

NSPCC Keeping Children Safe Online Safety and for Children with SEND

NSPCC Preventing online harm and abuse
Stop It Now! (UK and Ireland)

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

Social Media Guidance for parents and carers

Advice for parents and carers on cyberbullying

What to do if your child is a cyberbully | Internet Matters

NSPCC - Parental-controls

Internet Matters - Parental Controls

Digital Parenting Pro

Cerebra - Learning Disabilities, Autism and Internet Safety

Star Send toolkit

Ambitious about Autism – Online Safety

Child Protection Scotland - Online Abuse

OFG
Education