Online Safety Procedure

Our aim is to support students at St Piers to access the internet safely, prevent harm being caused to them online and respond to online safety concerns appropriately and sensitively.

CONTENTS

1. Purpose and Scope

For the intention of this procedure, 'online safety' is a term used to refer to how we use mobile devices, technology and the online environment safely. This includes the use of the internet and other means of communication using electronic media (e.g., text messages, gaming devices, email, and social media such as Facebook etc.). In practice, online safety is as much about behaviour as it is electronic security.

It is essential that our students are protected from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers us to protect and educate students and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

We know that the internet and associated devices, such as computers, tablets, mobile phones and games consoles are an important part of everyday life, which present positive and exciting opportunities, as well as challenges and risks.

We recognise that online safety is an essential part of safeguarding and acknowledge our duty to ensure that all students and staff are protected from potential harm online. We will empower our students to acquire the knowledge needed to use the internet and technology in a safe, considered and respectful way, and develop their resilience so they can manage and respond to online risks.

The purpose of the online safety policy is therefore to:

- safeguard and promote the welfare of students and staff online
- identify approaches to educate and raise awareness of online safety throughout the charity
- enable all staff to work safely and responsibly to role model positive behaviour online and to manage professional standards and practice when using technology
- identify clear procedures to follow when responding to online safety concerns
- protect the company from malicious attacks such as phishing, data leakage and data encryption.

This procedure applies to all access to the internet and use of technology, whether this is using personal or business devices and applies to all members of Young Epilepsy/St Piers (including staff, students, volunteers, parents/carers, visitors) who have access to and are users of digital technology systems.

2. Benefits and Risks

Digital technologies bring huge opportunities to learn, communicate, create and be entertained. For most people – and especially for children and young adults with disabilities –these benefits can outweigh the risks when used safely.

Benefits

- Inclusion and connection – Assistive technologies can help our students to communicate, make friends and connect with others, reducing isolation.
- Access to services – Online tools make activities such as shopping, banking, and education more accessible.
- Learning and creativity – The internet offers countless educational resources and creative outlets.

Risks

However, technology also carries risks that we must understand, teach about, and manage:

- Sleep disruption ('vamping'). Staying online late at night can harm attendance and learning.
- Online grooming. Offenders may pretend to be peers to exploit children or vulnerable adults sexually or criminally.
- Cyberbullying and trolling. Harassment via social media, messaging, or other platforms can be relentless due to 24/7 access.
- Inappropriate images. Threatening or indecent images may be taken, shared, or used for bullying, blackmail, or exploitation.
- Gang-related activity. Gangs can promote themselves or issue threats online, escalating violence and fear.
- Access to harmful content. Violence, pornography, pro-anorexia, self-harm, suicide, or hate sites.
- Radicalisation. Recruitment into extremist ideologies.
- Fraud and scams. Sharing personal details can lead to identity theft or financial loss.

Four Categories of Online Safety Risk

1. **Content** – Being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories. Exposure to illegal or harmful material (e.g., pornography, racism, misogyny, self-harm, extremism). The definition of content risks within online safety has now been broadened to encompass misinformation, disinformation (including fake news), and conspiracy theories.[1]
2. **Contact** – being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
3. **Conduct** – being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

[1] Educate Against Hate highlighted approaches to take within schools in this important area, and the Pears Foundation reported earlier this year that the best way to tackle misinformation, disinformation and conspiracy amongst young people is through schools

4. **Commerce** – risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/)

These risk areas are covered in Young Epilepsy/St Piers' Online Safety Training, reviewed annually or when legislation changes.

Common Technologies Used

- Internet
- Artificial Intelligence (AI)
- Email, instant messaging
- Blogs, vlogs, podcasts
- Webcams, video conferencing (Skype, Zoom)
- Social networking (Facebook, Twitter, Instagram, Snapchat, WhatsApp, TikTok)
- Location-based social networking
- Video platforms (YouTube)
- Chat rooms, forums, online gaming platforms
- Music download services
- Mobile phones with camera/video
- Applications ('apps').

See **Appendix 1** for more information on the different types of risk that exist for people using mobile devices, which we must be aware of, to help our students be wise to these and subsequently to avoid them.

3. National Legislation and Guidance

Our online safety work is shaped by the following current laws and official guidance:

- **Keeping Children Safe in Education (KCSIE) 2025** – The key government guidance for safeguarding in schools and colleges in England.
- **Online Safety Act 2023** – Requires online services to protect children and vulnerable people, including age checks, safer design features, and clear reporting options.
- **Children's Code (Age Appropriate Design Code)** – Sets privacy and design standards for websites, apps, and games likely to be used by under-18s.
- **Teaching Online Safety in Schools (DfE, 2019)** – Advice on how to teach pupils to stay safe online.
- **Working Together to Safeguard Children** – Guidance on how agencies work together to protect children.
- **Data Protection Act 2018 / UK GDPR** – Rules on collecting, storing, and sharing personal information safely.
- **Data (Use and Access) Act 2025** – Updates data protection law to cover new data-sharing, online identity checks, and research access.

- **Digital Economy Act 2017** – Includes rules on age checks for adult content and protecting copyright online.
- **Criminal Justice and Courts Act 2015** – Covers offences like revenge porn and malicious online activity.
- **Serious Crime Act 2015** – Includes offences for grooming, child sexual exploitation, and controlling/coercive behaviour.
- **Defamation Act 2013** – Protects people from false and damaging online statements.
- **Education Acts (2011, 2006)** – Set standards and duties for schools and colleges.
- **Equality Act 2010** – Protects against discrimination, including online.
- **Communications Act 2003** – Makes it illegal to send grossly offensive or threatening messages online.
- **Sexual Offences Act 2003** – Defines sexual offences, including those involving online contact.
- **Regulation of Investigatory Powers Act 2000** – Controls lawful monitoring of communications.
- **Human Rights Act 1998** – Protects rights such as privacy and freedom of expression.
- **Protection from Harassment Act 1997** – Covers harassment and stalking, including online.
- **Computer Misuse Act 1990** – Criminalises hacking and other unauthorised access to computers.
- **Malicious Communications Act 1988** – Makes it an offence to send threatening or grossly offensive messages.

4. Implementation of Procedures

We will take practicable steps to mitigate the risks involved with using the internet and mobile devices, to ensure that users create and access appropriate material. However, due to the enormity of internet content, it is also not possible to guarantee that students will never see inappropriate material, nor is it possible to prevent all concerning contact and conduct, due to the necessity to not over-restrict or inhibit internet use. We will however take the steps outlined below to reduce the risks as much as possible.

Student access to internet

Students can access the internet using organisational equipment or their own personal device/s.

If using a St Piers device, students must log-in using their own username and password which is provided when they start their placement. All such access will be filtered and monitored through the same system as all other organisational access (see section on Web Content Filtering).

If using any personal devices to access the internet (e.g., phone, game console, music console etc.), the device needs to be set up to access the internet via the IT Services Department. Access to the internet through any personal devices but using our Wi-Fi is also filtered and monitored through a separate network system. However, access to the internet through a mobile telecoms provider is not filtered or monitored.

The level of access for students will be determined through their risk assessment as completed by their teacher/tutor and house manager. Parents and carers (where appropriate depending on age and capacity of the student) will also be asked for their input into the development of such risk assessments and determining any necessary risk management actions.

By default, all students will have limited access, however when a risk assessment has been completed a student's access permissions may change to be more or less restrictive depending on the content of the risk assessment. The house manager, teacher or tutor should inform the IT team if a student needs to change their user group (e.g., an adult student has capacity and so needs to be placed in a different group to those who lack capacity to safely access the internet).

Risk Assessments

Each student must have a personalised Online Safety Risk Assessment that considers their specific needs and the potential risks associated with their use of the internet and digital technology. These assessments should be reviewed at least annually and shared with relevant individuals, including the student and their parents or carers where appropriate, to ensure transparency and a coordinated approach.

The teacher, tutor, or relevant manager is responsible for overseeing, implementing, and reviewing these assessments for their students. However, the Head of Service must ensure that robust auditing processes are in place to monitor compliance, consistency, and effectiveness across the service.

These assessments should aim to balance risk against benefit, ensuring students are not unnecessarily restricted from using digital technology while maintaining a safe online environment.

Online safety in the curriculum

Online safety is taught to all students as part of providing a broad and balanced curriculum, including as part of the requirements for Relationships Education and Relationships and Sex Education.

The subject of online safety has been mapped within the curriculum in school and within courses in college, and this subject area forms part of each student's learning. Staff support each young person in implementing learned safety strategies and how to report concerns where possible.

Online Safety is embedded within the home context by residential support staff. Students should be supported through everyday use of technology, keywork sessions and student meetings to cover the various elements of online safety and ensure there is practical application of what is learned in school or college. There are many creative resources available to support teams with differentiating this learning and making it appropriate for all children and young adults (see section 9 for some examples).

Remote/Home Learning

We will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements. Any new applications or tools being used by staff (such as video chat or social networking) must be discussed with the Head of IT prior to implementation to ensure that the risks of these are assessed and managed.

It is important that all staff who interact with students, including through online channels, continue to look out for signs that they may be at risk. Any such concerns should be dealt with as per our policy and where appropriate referrals should still be made to children's or adults social care and as required the police.

St Piers School and College should be mindful of contextual circumstances and how they may affect students and their parents/guardians/carers and take this into consideration when they are setting expectations of work at home.

If webcams/Skype etc. are to be used to deliver learning and/or keep in contact with parents/guardians/carers during this time the following needs to be considered:

- Staff and students must wear suitable clothing, as should anyone else in the household.
- Any computers used should be in appropriate areas and in communal areas – not in private bedrooms.
- Language must be professional and appropriate, including any parents/guardians/carers in the background.
- Staff must only use platforms agreed with senior leaders and the Head of IT to communicate with children and young people.

Staff must follow the Code of Conduct when communicating with students using the internet, social media or a mobile device. If staff are unsure about doing so, they must speak to their DSL.

Parents/carers can request resources from their child's teacher/tutor and access the St Piers website for guidance on how to keep their child/young person safe at home. This will be updated as appropriate.

Filtering

The IT department will apply appropriate technical and procedural controls to ensure that the school's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised

The organisation currently subscribes to Smoothwall, which applies filtering, monitoring and firewall solutions to the St Piers network. This applies when using the Wi-Fi and networked computers, whether it be students, staff or visitors.

Content in the following categories is blocked on our network:

1. Known malicious sites
2. Gambling
3. Piracy and copyright theft
4. Malware/hacking
5. Pro-self-harm, eating disorder or suicide content
6. Insecure shopping sites
7. Pornography
8. Terrorism and violence
9. Adult offensive content
10. Bullying

11. Drugs/substance misuse
12. Unapproved AI.

If staff or students find a legitimate web page necessary for daily tasks that are filtered, they will have the opportunity to request this page to be unblocked from the IT team. The IT Helpdesk require time to verify the authenticity of any specific website and to allow access.

Access to the web is via user groups as follows:

- Students under the age of 18 years
- Students over the age of 18 years with capacity
- Students over the age of 18 years without capacity
- Staff
- Visitors
- Staff who live on campus
- IT Staff

Students that are specifically risk assessed and require personalised access rules to the internet can be allocated personalised policies as required (as per their online safety risk assessment). Specific allowances that override or add sites within these categories can be configured.

Where a particular risk is identified for a student, their profile may need to be changed temporarily to protect them. The house manager/teacher/tutor must inform the safeguarding team and the IT team when they believe a change in the students' profile is necessary to safeguard them from harm.

The organisation will take all practicable measures to prevent access to inappropriate materials. Certain sites and programmes are deemed as prohibited (due to being illegal) and will not be available to any user.

Web Monitoring

The IT Department are responsible for the operation of Smoothwall and its monitoring of web access by all user groups. Alerts for students are sent daily to the Lead DSL and members of the online safety group. All breaches or attempted breaches need to be recorded on MyConcern®

Where concerns are raised through this, regarding staff conduct, these are immediately brought to the attention of the appropriate Head of Department, HR and the Lead DSL.

Staff training

At St Piers, we ensure that all staff working with students are trained in understanding online safety, during core induction and within their probationary period. The training covers the risks and benefits of internet access and technology use and support the staff to know what to do if they are concerned about a student's safety online and how to support students to use the internet and devices safely.

The trustees and governors are provided with updates relating to Online Safety through the board reports.

The safeguarding team and relevant members of the IT team will receive regular updates through events and reading materials/guidance relevant to online safety.

Communications

The St Piers email service may be regarded as safe and secure and is monitored. Staff must use their work email for professional matters only.

Users must immediately report, to a manager, the IT team or the DSL, the receipt of any communication that makes them feel uncomfortable, or that they feel is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

Any digital communication between staff to students or parents / carers (email, social media, chat, blogs etc.) must be professional in tone and content. These communications may only take place on official (monitored) St Piers systems. Staffs' personal email addresses, text messaging or social media must not be used for these communications.

Staff must always record details of any communications regarding students and parents in the appropriate system. Email should never be regarded as a filing system.

Social Media

Some students at St Piers choose to access social media. Students should only access social networking sites if they are old enough to have an account (e.g., to use Facebook you must be 13 years or over).

Students are given advice on security and privacy settings when using social networking sites by staff supporting them both in education and residential services.

As persons in a position of trust, staff should not befriend students on social networking sites. Further advice regarding this relationship is available in Young Epilepsy/St Piers Child and Adult Protection and Safeguarding Procedures and Code of Conduct.

Staff are required to familiarise themselves with St Piers' Social Media Guidance and act within this. It is important to be aware that even without engaging with students, ex-students, parents or carers on social media, they may still be able to access your information. Please ensure your settings are private. **Think before you post!**

It is important to realise that even the strictest privacy settings have limitations. This is because, once something is online, it can be copied and redistributed. If you are unsure whether something you post online could compromise your professionalism or your reputation, you should think about what the information means for you in practice and how it affects your role as a person in a position of trust. It is also important to consider who and what you associate with on social media, acknowledging someone else's post can imply that you endorse or support their point of view. You should consider the possibility of other people mentioning you in inappropriate posts. If you have used social media for a number of years, it is important to consider, what you have posted online in the past.

Staff should also ensure that:

- No reference should be made in social media to students, parents/carers or staff.
- They do not engage in online discussion on personal matters relating to members of the Charity's community.

- They do not share images or memes etc. which may compromise their professional status and the reputation of the Charity.
- Personal opinions should not be attributed to the Charity.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- They must never use student devices for their own purposes and/or use their own log in on a student device.

Staff personal use:

- Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with the Charity or impacts on the Charity, it must be made clear that the member of staff is not communicating on behalf of the Charity with an appropriate disclaimer. Such personal communications are within the scope of this policy.
- Personal communications which do not refer to or impact upon St Piers are outside the scope of this procedure.
- Where excessive personal use of social media at work is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.

Emerging Technologies

The appropriate use of learning platforms will be discussed as the technology becomes available within the educational settings, with regular reviews regarding their impact, use and efficacy.

Photography and Videos

Digital imaging technologies bring many benefits for learning, maintaining relationships, and social interaction. However, staff, parents/carers and students must be aware of the risks of publishing digital images online. Once shared, images may remain accessible indefinitely and could lead to cyberbullying, grooming, or cause harm and embarrassment in the short or long term.

Staff should educate students about the risks associated with taking, using, sharing, and distributing images, and should be familiar with the Information Governance guidance on photography.

Photographs or videos of students must only be taken using a Young Epilepsy/St Piers device. The necessary consent must always be obtained before taking an image, and if a student has the capacity to consent, their decision must be recorded whether they agree or decline.

Images must have a clear professional purpose. No inappropriate or potentially misinterpreted photographs are permitted. Staff must never take photographs of a student in a state of undress, in underwear, or nude.

Care must be taken when saving and distributing images. Photographs of students must only be emailed from a Young Epilepsy/St Piers email account, with a clear explanation for their use, and always within the scope of the consent given. All images must be securely stored on the Young Epilepsy/St Piers network.

Managers are responsible for ensuring systems are in place to check and delete photographs from devices at least weekly.

The physiotherapy team take photographs of students in their spinal clinic. These photographs are taken with a St Piers device and explicit consent is always gained and recorded for these purposes. Please see the **Therapy Photographing of Injuries Procedure** for further information. These photographs will show students with their spine exposed (therefore with no clothing on their torso) but with their lower body clothed. The physiotherapist is responsible for ensuring that any such photographs taken are stored safely and only the necessary therapists have access to these photographs. If the photographs need to be distributed to staff teams, there must be a clear rationale for this and an accompanying statement to the receiving staff, about what the purpose of these photographs is and that the images must under no circumstances be distributed further.

The safeguarding team or medical professionals may, in exceptional circumstances, be required to take photographs of injuries or bruising on students. Such photos must only be taken on a St Piers device and by someone within the medical team. Due caution must be taken with regards to the parts of the body captured within the image and how the image is shared and stored. Advice should be sought from the Head of Safeguarding and Quality in such instances.

Mobile Phones

All staff must agree to and sign the Code of Conduct, this is a mandatory document, which outlines the guidance for personal mobile phone use. Staff who are found to be using the internet or any mobile devices in an inappropriate, illegal or harmful way may be subject to action under the disciplinary policy and procedures. Staff must read and act as per the guidance outlined in the IT policy and procedure.

Where students have mobile phones, staff must ensure that students are supported to use their devices safely and appropriately. The Student Agreement provides guidance to students about their roles and responsibilities around use of mobile phones. Students must not use mobile phones whilst in lessons at school or college and follow the rules for each area. Like in any other parents/guardians/carers setting, there may also be occasions when there are agreed deadlines set for students to use their phones and any other personal mobile devices.

See Young Epilepsy/St Piers' Use of Mobile Devices Procedure for more information.

Support for Parents and Carers

Some parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

We will therefore provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters and the web site,
- High profile events/campaigns e.g., Safer Internet Day
- Reference to the relevant web sites/publications e.g., swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers.

5. Roles and Responsibilities

Trustees

The Trust Board has overall responsibility within Young Epilepsy/St Piers for safeguarding the children and young adults that are supported by the organisation. This includes, safeguarding them from online risks. The Trust Board should ensure that Governors monitor the effectiveness of the curriculum around online safety.

Governors

KCSIE 2025 states (128):

Governing bodies and proprietors should ensure that children are taught about how to keep themselves and others safe, including online. It should be recognised that effective education will be tailored to the specific needs and vulnerabilities of individual children, including children who are victims of abuse, and children with special educational needs and/or disabilities (SEND).

Subsequently, the Education Governing Body are responsible for ensuring that there is compliance with the above, through challenge and monitoring of the school, college and residential special schools houses.

IT Team

The Head of IT ensures that the technical infrastructure at Young Epilepsy/St Piers is not open to misuse or attack and that the organisation is compliant with online technical requirements. They are responsible for the day-to-day management of information security activities and responding to Information Security Incidents.

The IT team will provide access for all students as advised by the senior management team. They will also provide reports on student usage when requested.

The IT Helpdesk will additionally support student personal device's access and connect to Young Epilepsy/ St Piers' systems; the working condition of personal hardware and software is the responsibility of the person.

Further to this the Head of IT will support the safeguarding team to understand and manage filtering and monitoring systems and carry out regular reviews and annual checks.

Online Safety Coordinators

We have an online safety group who meet regularly and are key members of staff with regard to implementing and ensuring good practice who are responsible for:

- Developing a safe culture with regards to use of technology
- Being the main point of contact on issues relating to online safety
- Raising awareness and understanding of online safety issues amongst staff and parents and carers
- Keeping up with relevant online safety legislation
- Supporting the Lead DSL and Head of IT to update policies, procedures and provide training related to online safety.

Education and Residential Services Senior Management

As the persons responsible for the care and education of the learners, the senior management teams of the education and residential services departments should ensure that:

- All students in their care are given access to technology as appropriate.
- Risk assessments for their students are carried out, reviewed and are appropriate for the needs of the specific learner.
- Staff and student access in their departments is monitored and any actions needed are followed up appropriately.
- Staff attend training on online safety.

Safeguarding Team

- All staff are responsible for reporting any suspected concerns regarding the safety and wellbeing of a student, or the worrying behaviour of an adult to a member of the Safeguarding Team at the earliest opportunity.
- Where there is a concern of a student accessing or being at risk of accessing harmful or inappropriate content, or are being abused or harmed through technology, staff must report this immediately to the DSL. They will respond appropriately to all incidents or devolve actions as necessary.
- The DDSL must liaise with the Head of IT/Lead DSL to ensure they are appraised of the situation and to seek advice as appropriate.
- The Lead DSL works with the Head of IT to ensure the monitoring and filtering systems across the site are appropriate and as effective as possible.

All Staff

All staff have a duty of care to all the children and young adults that are supported by the organisation. This duty of care involves safeguarding students and so all staff must:

- Ensure that they have an up-to-date awareness of online safety matters and the Online Safety Policy and Procedures.
- Read, understand and follow the Code of conduct for staff and IT Acceptable Use agreement.
- Report any concerns about online safety to the safeguarding team.
- Help students they support to understand how to stay safe online.
- Role model safe and positive use of technology and the internet.
- Report any concerns relating to online safety immediately as per this procedure and the Child and Adult Protection and Safeguarding Procedure.

Tutors/Teachers and Senior House Managers/House Managers

As the persons responsible for the day-to-day planning, reviewing and management of learner activities, the tutor/teacher and unit manager for each learner must ensure that:

- Staff in their area are fully aware of their responsibility and how to implement the policy through training and guidance.

- A risk assessment for each student is carried out and communicated to all relevant members of staff when appropriate, parents and carers are informed of the outcome of the risk assessment and the impact of this on the student's access is explained.
- The IT Department is informed when a student's access to the internet does not fall in to the 'typical' user group or where personalised access is required.
- Students are supervised and the appropriate services informed of any breaches of the policy.
- Online safety issues are embedded in all aspects of the curriculum and other activities.
- They monitor the use of digital technologies, mobile devices, cameras etc. and implement current policies with regard to these devices.

Information Governance Steering Group

The Information Governance Steering Group has delegated authority from the Chief Executive, for the implementation and annual review of Young Epilepsy/St Piers' Information Technology Policies and governance, and for re-issuing them each year following their approval by the Executive.

Visitors

Young Epilepsy/St Piers provide a free guest Wi-Fi network for visitor use. Guest Wi-Fi is subject to the same filters as the corporate network. All visitors must be informed that traffic is monitored on the guest Wi-Fi.

6. Data Protection

At Young Epilepsy/ St Piers, personal data is recorded, processed, transferred and made available according to the current data protection legislation.

All staff when using IDMT's (Internet Digital and Mobile Technologies) must apply the following policies and procedures and their associated guides:

- Confidentiality Policy and Procedure
- Data Protection Policy and Procedures
- Information Governance Policy and Procedures
- Information Risk Management Policy and Procedures

These documents specify how information may be used, transferred or disclosed and can be found on the intranet.

7. Reporting and Monitoring

If staff or students discover unsuitable sites, they will be required to alert an appropriate person immediately. The member of staff will report the concern (including the URL of the site if possible) to the Head of IT/Lead DSL. The breach will be recorded and escalated as appropriate.

If a student's internet use and their safety is in question, staff must notify the appropriate DSL. If appropriate, a request can then be made by the DSL to the IT team to access a log of the student's

online activity to see whether they are at risk of significant harm and put measures in place to protect them.

In the event of a major cyber-attack or ransomware incident, staff should follow the organisation's Cyber Incident Response Plan and notify the Head of IT immediately.

Any material that we believe is illegal will be reported immediately to the appropriate agencies, such as Internet Watch Foundation (IWF), the Police or Child Exploitation and Online Protection (CEOP).

This procedure will be reviewed annually and as required in the light of any significant new technological developments, new threats to online safety or incidents that have taken place.

Staff will be asked to evaluate the effectiveness of the procedures whenever they have had occasion to put them into practice.

8. Procedure for Managing Prohibited and Inappropriate Internet Use

Some internet activity is illegal and strictly prohibited at Young Epilepsy / St Piers. This includes, but is not limited to, accessing child abuse images, engaging in cyberbullying, or distributing racist material.

Other activities, while not necessarily illegal, may still be inappropriate within Young Epilepsy/St Piers depending on the ability and capacity of the student. Examples are provided in Appendix 3.

Any online safety concerns raised by staff, students, volunteers, or parents must be reported immediately to a DSL. The DSL will liaise with external agencies as appropriate, which may include:

- The police, where illegal activity is involved (such as indecent images of children or adult material that breaches legislation)
- Children's Social Care, where a child's vulnerability requires referral
- Adult's Social Care, where an adult's vulnerability requires referral
- The Local Authority Designated Officer (LADO), if the alleged perpetrator is a professional
- Parents/carers, where appropriate
- Action Fraud, the national fraud and cyber-crime reporting centre.

Where necessary, evidence related to the concern may need to be preserved. In such cases, equipment may be taken temporarily, following advice from the Head of IT.

If staff suspect that indecent images of children have been taken, produced, or received, they must avoid viewing the content wherever possible. Under no circumstances should they attempt to copy or save such imagery. The DSL should be alerted immediately, and if the content was accessed online, the website URL should be noted.

Any concerns relating to online safety involving students must be recorded on MyConcern®

9. Useful Resources

The following resources can be used to educate students and staff on the safe use of the internet and internet related technologies:

The following sites provide information and support to help students, staff and parents get the most out of the internet whilst staying safe:

1. ThinkUKnow – Resources for Teachers, Parents and Young People
2. UK Council for Internet Safety (UKCIS) Education for a connected world
3. NCA-CEOP – Child Exploitation and Online Protection Centre
4. Internet Watch Foundation
5. UK Council for Child Internet Safety (UKCCIS)
6. Childnet International
7. UK Safer Internet Centre
8. Net Aware
9. BBC Own It
10. Parentzone
11. Kidsmart
12. Mencap- Parent's guide to internet safety
13. Young Minds
14. Childline – 0800 1111
15. Action Fraud
16. The professionals Online Safety Helpline (POSH)
17. Internet Matters
18. NSPCC
19. UKIS – Sharing nudes and semi-nudes: advice for education settings working with children and young people
20. NSPCC Report Remove: A free, confidential service for young people under 18 to report and remove sexual images or videos of themselves shared online. The tool works with the Internet Watch Foundation (IWF) to take down illegal content and provides support via Childline. Childline's Report Remove page.

Version Table

This policy is agreed by the Trust Board and will be implemented by all departments.	
Signed:	**Date:**
Position:	**Reviewed 31 August 2025** **Next review 01 September 2026**

Version table			
Creation: - Gill Walters **Approved by: - xxxxx**			
Version No.	**Date of changes**	**Reason for change**	**Changes made by**
2	31 Aug 2022	General review/minor amendments in line with KSCIE 2022	Gill Walters
3	31 Aug 2023	Annual review/ amendments in line with KSCIE 2023	Gill Walters
4	31 Aug 2024	General review/minor amendments in line with KSCIE 2024/Working together Addition of AI/Sextortion Addition to FAQ Appendix 2 – Q 11	Gill Walters
5	14 August 2025	Annual review/ amendments in line with KSCIE 2025 Updates to Four Categories of Online Safety Risk (pg. 3 & 4) Review and re – format of FAQ – Appendix 2	Gill Walters

Appendix 1- Types of Online Risks

Cyber Bullying

Cyber bullying is as serious as face-to-face bullying and can happen anytime, anywhere, making it hard for victims to escape. It can invade safe spaces, go unnoticed, and cause severe emotional harm, including self-harm or suicide in extreme cases.

It often involves groups targeting individuals, and actions that seem harmless – such as negative comments on a photo – can quickly escalate. Children with special educational needs are at much higher risk.

The following are the most commonly reported ways in which bullying occurs:

- **Email** – Used to send derogatory or prejudiced comments, harassment, or harmful images to individuals or groups, sometimes escalating from what was intended as a joke.
- **Instant Messaging / Chat Rooms** – Direct or group messages that can escalate quickly; may involve grooming or requests for inappropriate images from people posing as someone else.
- **Social Networking Sites** – Fake profiles, harmful posts, and non-consensual images can be used to target individuals; grooming risks are also present.
- **Mobile Phones** – Anonymous abusive calls, texts, or media sharing, including criminal sharing of attack videos; internet access on phones increases exposure to harmful content and privacy risks.
- **Interactive Gaming** – Players may be abused, threatened, groomed, excluded from games, or have accounts hacked; false rumours may be spread.
- **Viruses / Hacking** – Used to damage devices or steal/delete personal data.
- **Abuse of Personal Information** – Sensitive content posted online without consent, accounts hacked, or impersonation.

It is important that staff are clear with students about expected conduct whilst in education and at home, and that bullying behaviour is unacceptable and will be dealt with seriously by the organisation.

Fraud and cybercrime

There are many words used to describe fraud: scam, con, swindle, extortion, sham, double-cross, hoax, cheat, ploy, ruse, hoodwink, confidence trick. Fraud can be committed against individuals or businesses.

Cybercrime is any criminal act dealing with computers and networks (called hacking). Additionally, cybercrime also includes traditional crimes conducted through the Internet.

There were 3.8 million frauds and 2 million cybercrimes last year – based on survey results from the Office for National Statistics (ONS).

Children and young people can be more at risk from fraud and cybercrime due to being unaware of such risks and being naive to other's sinister intentions. People with learning disabilities can therefore also be very vulnerable to such crime, and it is important that we help educate those that we support to be more aware of the risks and how to avoid them.

Trolling

Trolling is the deliberate act of provoking others online through hatred, bigotry, racism, misogyny, or disruptive arguments. Trolls use any platform that allows public comments, such as social networks, news sites, forums, blogs, or game chats.

While trolling and cyberbullying are related, they differ: cyberbullying targets a specific individual repeatedly, whereas trolling aims to provoke anyone to get a reaction, often without a personal motive.

Trolling is an offence under the Malicious Communications Act, but identifying offenders can be difficult.

Prevention and response:

- **Ignore** – Do not reply to offensive or immature comments, as this encourages the troll.
- **Block** – Remove their access and block them again if they reappear.
- **Report** – Notify website administrators each time they return under a different name.

Indecent images of children

Most indecent images of children (under 18) are created by adults, which constitutes abuse. However, some are created by children or young people themselves. Youth produced sexual imagery includes:

- A person under 18 creating and sharing a sexual image of themselves with another person under 18.
- A person under 18 sharing a sexual image made by another child or by an adult.
- A person under 18 possessing a sexual image created by another child.

Young people may produce such imagery due to risk-taking, peer pressure, or increased sexual awareness. The prevalence of smartphones, internet access, and Bluetooth means images can be shared instantly, often without considering the consequences.

This is commonly known as **"sexting"** and can have serious, lasting harm. Once online, images can be copied, altered, or shared widely, sometimes falling into the hands of predatory abusers. An Internet Watch Foundation study found 88% of self-taken sexual images of young people were taken from their original location and reposted elsewhere.

It can be difficult to distinguish between images created through grooming by adults and those resulting from peer experimentation. Under UK law (Protection of Children Act 1978 and Sexual Offences Act 2003), it is illegal to take, make, distribute, show, or possess indecent images of anyone under 18. This includes youth produced sexual imagery. However, UK Council for Child Internet Safety (UKCCIS) guidance supports proportionate handling to avoid criminalising children unnecessarily.

When such imagery is discovered, Young Epilepsy/St Piers will treat it as a safeguarding concern. Referrals will be made to Surrey Children's or Adult's Services, and the police may be involved if a crime is suspected.

‘Revenge Pornography’

Under the Criminal Justice and Courts Act 2015, it is a criminal offence to disclose private sexual photographs or films with intent to cause distress. This applies both online and offline, including uploading images to the internet, sharing via text or email, or showing physical or electronic copies.

While often linked to people in a current or former physical relationship, revenge pornography can also occur through online grooming, where strangers coerce or blackmail individuals into providing self-taken sexual images. Young people must be supported to recognise the risks of being approached by strangers on social media or through phishing emails, and to know how to respond.

All young people should understand the risks of allowing someone to take an indecent photograph or video of them. Any instance of a student being a victim or perpetrator of revenge pornography must be reported as a safeguarding concern.

Grooming

Grooming is the process by which someone prepares a child, their caregivers, and the environment to abuse the child. This includes gaining access, compliance, and secrecy to avoid detection.

Online grooming is common: perpetrators can hide their identity, manipulate trust, and exploit children who may overshare information online.

Under the Serious Crime Act 2015:

- It is an offence for an adult to communicate sexually with a child under 16 or to elicit a sexual response.
- It is illegal for an adult to arrange to meet a child under 16 after any sexual communication.

Schools must treat any suspected grooming as a safeguarding concern and report it to a DSL.

Artificial Intelligence (AI) Risks and Sextortion

There are new developments which staff should be aware of:

Virtual Reality (VR) and Metaverse Safety – These environments have unique safeguarding challenges (realistic avatars, private virtual rooms, immersive grooming). Staff should be aware of the risks and follow agreed safety protocols before allowing student access.

Live Streaming Risks – Explicit guidance should be given on the use of live streaming platforms (e.g., TikTok Live, Twitch) including privacy settings, supervision, and how to respond to inappropriate contact.

End-to-End Encrypted Messaging Apps – Staff should note the safeguarding limitations of apps such as WhatsApp, Signal, and Telegram due to monitoring restrictions. Online risk assessments should reflect any use of these tools by students.

AI Use by Staff – Staff must not input personal or sensitive data into public AI tools and should follow ICO guidance on responsible AI use in educational contexts.

What is AI?

AI uses computer systems to solve problems and make decisions. Generative AI (GenAI) can create text, images, or videos from prompts. Common tools include:

- Text: ChatGPT, Google Gemini, GrammarlyGO
- Images/Videos: DALL-E, Midjourney

AI is rapidly evolving, producing more realistic content, including abusive, pornographic, or illegal material. Some chatbots and apps encourage harmful behaviour, bullying or self-harm.

AI can exacerbate existing safeguarding issues:

- Misinformation and Scams: AI-generated text can create convincing phishing emails or messages.
- Child Sexual Exploitation: AI can produce sexualised images or deepfake pornography of children.
- Catfishing and Sextortion: Criminals may use AI-generated profiles to groom or coerce young people into sending sexual images.
- Addictive or Harmful Tools: Unmoderated AI apps may blur reality or encourage inappropriate content creation.

What is Sextortion?

Sextortion is financially motivated sexual blackmail, often by adults or organised crime groups.

Offenders may:

- Pose as peers or adults to groom children online
- Coerce children into sending sexual images
- Use stolen or AI-manipulated images to demand money or favours.

Key Safeguarding Actions

- Educate students on AI risks and sextortion
- Encourage reporting of suspicious contacts or coercion
- Monitor online platforms and digital tools used by students
- Treat any sextortion case as a safeguarding concern and involve the DSL.

Appendix 2: Frequently Asked Questions

Question	Answer
Q1. Can I add students as friends on social networking sites?	No. This blurs professional boundaries and may lead to inappropriate relationships. The same applies to former students. Staff must use strict privacy settings and, if social networking is used in the curriculum, support students via separate, approved accounts.
Q2. Can I add students' parents as friends on social networking sites?	No. Any pre-existing personal relationship should be disclosed to your manager.
Q3. I'm concerned about a colleague's social media activity. What should I do?	Report to your line manager. Refer to safeguarding and whistleblowing procedures.
Q4. Can I connect my personal device to the organisation's Wi-Fi?	Yes, responsibly. IT monitors usage – misuse may result in suspended access.
Q5. I received an email from an unknown source. What should I do?	Assume it is harmful and delete it. Report if unsure.
Q6. Can students over 18 access explicit adult content?	Accessing adult content is legal from the age of 18. However, for students with additional needs, it may be confusing or harmful. Students should receive tailored guidance on safe use, understanding consent, respecting boundaries, and maintaining privacy online. Any access should be supported and monitored appropriately to ensure it does not cause distress or exploitation.
Q7 What is inappropriate material?	Anything Illegal: Child sexual abuse images, sexual activity with animals, necrophilia, acts Inappropriate but legal: Actions that breach professional boundaries or bring the organisation into disrepute (e.g., posting offensive comments about students or colleagues online).
Q8. What signs might indicate a student is at risk online?	Look for: • Spending unusually long or short time online • Tiredness or disrupted sleep • Emotional outbursts linked to device use • Secretive behaviour about online activity.
Q9. What is deepfake content and why is it a risk?	Deepfakes manipulate images, videos, or audio to falsely represent someone. They can be used for sexual exploitation, bullying, or spreading misinformation.

Question	Answer
Q10. How should staff respond to online abuse or cyberbullying?	Report incidents to a line manager or DSL. Preserve evidence but do not forward or respond. Follow safeguarding procedures.
Q11. Can students use AI tools ?	AI can expose students to unsafe content, misinformation, and grooming. Students to be taught how to: • Recognise harmful AI-generated content • Avoid sharing personal information • Report unsafe content.
Q12. How can students protect themselves online?	Teach students to: • Keep personal information private • Use strong passwords • Enable privacy settings • Avoid sharing with strangers • Report suspicious messages or contacts.
Q13. What is fake news?	Fake news is false or misleading information presented as if it were real news. Images might be edited or taken out of context. Reverse image search can help spot fakes. Use sites like **Snopes**, **PolitiFact**, or **BBC Reality Check** to confirm.

Appendix 3: Overview of the acceptability of online behaviour

The following table provides an overview of the acceptability of online behaviour:

		Acceptable at specific times	Acceptable for nominated users	Unacceptable	Illegal
Users Sharing	Child sexual abuse images- making, producing and distributing				X
	Grooming				X
	Possession of 'extreme' pornographic imagery				X
	Criminally racist material				X
	Pornography accessed by staff at work			X	
	Legal pornography accessed by students	X	X		
	Promotion of extremism or terrorism				X
	Promotion of any kind of discrimination			X	X
	Threatening behaviour including promotion of physical violence or mental harm			X	X
	Any other information that may be offensive to colleagues or breaches the integrity of the charity or brings the Charity into disrepute.			X	
Using systems, applications, websites or other mechanisms that bypass filtering by the Charity				X	

	Acceptable at specific times	Acceptable for nominated users	Unacceptable	Illegal
Infringing copyright			X	
Revealing or publicising confidential information about the Charity, staff or students			X	
Intentionally creating or propagating computer viruses or other harmful files or applications			X	X
Online gambling – students	X	X		
Online gambling – staff at work			X	
Online shopping/commerce – students	X			
Personal online shopping/commerce – staff at work			X	
Use of social media, social networking, messaging apps or video broadcasting- students	X	X		
Use of social media, social networking, messaging apps or video broadcasting – staff at work	X			