Online Safety Procedure

Our aim is to promote the safe and responsible use of digital technology across Young Epilepsy and St Piers, protect children, young people and adults at risk from online harm, and ensure that online safety concerns are identified, reported and responded to appropriately and sensitively.

CONTENTS

1. Purpose and Scope 2
2. Benefits and Risks 3
3. National Legislation and Guidance 5
4. Implementation of Procedures 6
5. Roles and Responsibilities 15

Information Governance Steering Group 20

Visitors 20

6. Data Protection 21
7. Reporting and Monitoring 21
8. Procedure for Managing Prohibited and Inappropriate Internet Use 22
9. Useful Resources 23

Version Table 24

Appendix 1- Types of Online Risks 26

Appendix 2: Overview of the acceptability of online behaviour 34

1. Purpose and Scope

For the purposes of this procedure, *online safety* refers to the safe and responsible use of mobile devices, technology and online environments. This includes the use of the internet and other forms of electronic communication, such as email, text messaging, gaming platforms, social media and emerging technologies. Online safety is as much about behaviour and safeguarding as it is about technical 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 staff to protect and educate students in their use of technology and establishes clear mechanisms to identify, respond to and escalate concerns where appropriate

We recognise that the internet and digital technologies play an important role in everyday life and can provide valuable opportunities for learning, communication, independence and social connection. However, they also present potential risks which must be understood and managed.

We recognise that online safety is an essential part of safeguarding and acknowledge our duty to ensure that students, staff and others who access our systems are protected from harm online. We aim to equip students with the knowledge, skills and support required to use technology safely, responsibly and respectfully, whilst developing their resilience and ability to respond to online risks.

The purpose of this procedure is to:

- Safeguard and promote the welfare of students and staff online.
- Raise awareness and understanding of online safety across the organisation.
- Enable staff to work safely, responsibly and professionally when using digital technology.
- Establish clear procedures for recognising, reporting and responding to online safety concerns.
- Support the safe use of technology whilst reducing risks associated with cyber security threats, including phishing, malware, ransomware and data breaches.

This procedure applies to all use of the internet and digital technology, whether accessed through organisational or personal devices. It applies to all members of the Young Epilepsy & St Piers community, including students, staff, volunteers, parents and carers, visitors, supporters, service users and contractors who access or use organisational systems or networks.

2. Benefits and Risks

Digital technologies provide significant opportunities to learn, communicate, create and participate in society. For many people, and particularly children and young adults with disabilities, the benefits of technology can greatly enhance independence, communication, learning and social inclusion when used safely.

Benefits

- **Inclusion and communication** – Assistive technologies can help students communicate, build relationships and reduce social isolation.
- **Access to services** – Online tools can improve access to education, healthcare, information, shopping and other services.
- **Learning and creativity** – Digital technology provides opportunities for learning, problem-solving, self-expression and creativity.
- **Independence and life skills** – Technology can support students to develop independence, make informed choices and participate safely in their communities

Risks

Technology also presents risks which staff, students, parents and carers need to understand and manage appropriately. These may include:

- **Sleep disruption ('vamping')** – Excessive use of technology, particularly at night, can affect sleep, wellbeing, attendance and learning.
- **Online grooming and exploitation** – Offenders may target children, young people and vulnerable adults for sexual, criminal or financial exploitation.
- **Cyberbullying and online harassment** – Abuse through social media, gaming platforms, messaging applications or other online services can be persistent and difficult to escape.
- **Inappropriate, indecent or manipulated images** – Images may be created, altered or shared to bully, exploit, blackmail or harm others.
- **Exposure to harmful content** – This may include violence, pornography, self-harm, suicide, hate-based content, misinformation, disinformation and extremist material.
- **Radicalisation and extremism** – Online platforms can be used to expose individuals to extremist ideologies and harmful influences.
- **Fraud, scams and financial exploitation** – Personal information may be used for identity theft, financial abuse or other criminal activity. [
- **Artificial intelligence (AI) and emerging technologies** – AI-generated content, deepfakes, misinformation and online manipulation may increase safeguarding risks.

Four Categories of Online Safety Risk

1. **Content** – Being exposed to illegal, inappropriate or harmful content, for example: pornography, racism, misogyny, the promotion of violence against women and girls (VAWG), harmful gender stereotypes, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories. Exposure to online content that promotes harassment, abuse, coercive behaviour or image-based abuse should be treated as a safeguarding concern and responded to in line with safeguarding procedures. See Appendix 1 for further guidance.
2. **Contact** – being subjected to harmful online interaction with other users. This may include peer pressure, bullying, harassment, unwanted contact from strangers, commercial exploitation, and adults posing as children or young people in order to groom, manipulate or exploit them for sexual, criminal, financial or other purposes.
3. **Conduct** – personal online behaviour that may increase risk to an individual or others. This includes cyberbullying, sharing inappropriate or sexualised content, image-based abuse, uploading or forwarding harmful material, unsafe use of social media, online harassment, participation in harmful online challenges, and behaviour that may place the individual or others at risk of harm.
4. **Commerce** – risks associated with online financial activity, including online gambling, phishing, scams, financial exploitation, identity theft, misleading advertising, unauthorised purchases, and the misuse of personal or financial information. Students and staff should be supported to recognise and report suspicious online activity. Concerns relating to fraud, phishing or cybercrime should be reported through organisational safeguarding and IT reporting processes.

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
- Video conferencing platforms (e.g. Microsoft Teams, Zoom)
- Social networking platforms (e.g. Instagram, TikTok, Snapchat, Facebook, WhatsApp and Bluesky)

- 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) 2026** – Statutory safeguarding guidance for schools and colleges in England. Online safety is a safeguarding issue and includes protecting children from online risks associated with content, contact, conduct and commerce, including risks arising from artificial intelligence, online abuse, misinformation and emerging technologies.
- **Online Safety Act 2023** – The Online Safety Act places duties on online platforms to reduce children's exposure to illegal and harmful content, implement age-assurance measures where required, and provide effective reporting and moderation systems. Staff should support students to understand age restrictions, reporting tools and online safety features available on platforms they use.
- **Protection of Children Act 1978** – Creates offences relating to the taking, making, possession and distribution of indecent images of children.
- **Voyeurism (Offences) Act 2019** – Introduced specific offences relating to upskirting and non-consensual image capture.
- **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 relating to image-based sexual abuse, including the non-consensual disclosure of intimate images.
- **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 all reasonable and practicable steps to reduce the risks associated with the use of the internet and digital technology and to support safe and appropriate online behaviour. However, due to the scale and constantly evolving nature of online content and communication, it is not possible to guarantee that students or service users will never encounter inappropriate material or experience harmful online interactions. It is also important that online safety measures do not unnecessarily restrict access to the educational, social and assistive benefits that technology can provide. We will therefore take the steps outlined below to minimise risks and promote the safe, responsible and positive use of technology.

Student access to internet

Students can access the internet using organisational equipment or their own personal devices.

Students may use personal devices (for example, mobile phones, tablets, games consoles or music devices) to access the organisation's Wi-Fi network. Access to the Wi-Fi network requires the user's organisational username and password where applicable. Internet traffic accessed through the organisation's Wi-Fi network is subject to the organisation's filtering arrangements. However, internet access through a mobile telecommunications provider (for example, 4G or 5G mobile data) is not subject to the organisation's filtering systems. Monitoring arrangements apply only to supported organisational systems and devices and do not extend to all personal devices connected to the Wi-Fi network.

The level of internet access available to each student will be determined through their online safety risk assessment, completed by their teacher/tutor and House Manager. Parents and carers, where appropriate and taking account of the student's age, capacity and understanding, should be involved in the development and review of these assessments.

Risk assessments should consider the student's individual needs, vulnerabilities, understanding of online relationships, ability to recognise online risks, and capacity to use technology safely. The aim is to achieve an appropriate balance between safeguarding and access to the educational, social and assistive benefits that technology can provide.

By default, students will be allocated an access profile appropriate to their age and circumstances. Internet access may be increased or restricted following completion or review of a risk assessment. Where a student's access requirements fall outside standard arrangements, the House Manager, teacher or tutor must inform the IT Team so that appropriate user groups, filtering or monitoring controls can be applied.

Risk Assessments

Each student must have a personalised Online Safety Risk Assessment that considers their individual 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, where appropriate, their parents or carers, to support a coordinated approach to online safety.

Risk assessments should consider the student's understanding of online relationships, consent, privacy, information sharing, financial exploitation and their ability to recognise manipulation, coercion or deception online. Particular consideration should be given to

students whose disability, communication needs, cognitive profile or vulnerability may increase their risk of online harm.

The teacher, tutor or relevant manager is responsible for developing, implementing and reviewing these assessments. Heads of Service are responsible for ensuring that robust auditing and quality assurance processes are in place to monitor compliance, consistency and effectiveness across their service.

These assessments should aim to balance risk against benefit, ensuring that students are not unnecessarily restricted from accessing the educational, social, communication and independence-promoting benefits of digital technology, whilst maintaining a safe online environment.

Online safety in the curriculum

Online safety is taught to all students as part of a broad and balanced curriculum, including through Relationships Education, Relationships and Sex Education (RSE) and Preparation for Adulthood pathways where appropriate.

Online safety is embedded within the school and college curriculum and forms part of every student's learning. Staff support students to develop and apply online safety skills, understand risks and know how to seek help or report concerns where possible.

Students should be supported, at a level appropriate to their age, understanding, communication needs and vulnerabilities, to recognise that content encountered online may not always be genuine. This includes understanding that artificial intelligence (AI) can generate realistic images, videos, audio and text that may be misleading, inaccurate or created to deceive, manipulate or exploit others.

Online safety is also embedded within residential provision. Through the everyday use of technology, key working sessions and student meetings, students should be supported to develop the knowledge and skills needed to use technology safely and responsibly and to apply their learning in real-life situations. Resources should be adapted where necessary to ensure they are accessible and appropriate for individual learners.

Remote/Home Learning

Any use of online learning platforms, communication tools or digital systems must comply with data protection and information governance requirements. Any new application or platform proposed for use with students must be approved by the Head of IT before implementation to ensure that privacy, safeguarding and security risks have been appropriately assessed and managed.

All staff who interact with students or service users through online channels must remain alert to signs that a student may be at risk of harm. Any concerns must be responded to in accordance with safeguarding procedures and, where appropriate, referrals made to Children's Social Care, Adult Social Care or the Police.

When planning remote or online learning activities, staff should take account of the individual circumstances, needs and vulnerabilities of students, service users and their families, including any barriers to accessing technology or online learning

Where video conferencing or online communication platforms (e.g. Microsoft Teams, Zoom or equivalent approved platforms) are used to deliver learning or maintain contact with students and families, the following must be considered:

- Staff and students must wear appropriate clothing, as should anyone else visible in the environment.
- Devices should be used in appropriate locations wherever possible and not in private or unsuitable settings.
- Language and behaviour must remain professional and appropriate at all times.
- Staff must only use platforms approved by senior leaders and the Head of IT to communicate with students and families.

Staff must follow the Code of Conduct when communicating with students using digital technology, social media or mobile devices. If staff are unsure whether a communication is appropriate, advice should be sought from the DSL/DSO before proceeding

Parents and carers may request resources from their child's teacher or tutor and can access information and guidance through the St Piers website to support online safety at home. Resources and advice will be reviewed and updated as required

Filtering & Monitoring

Young Epilepsy/St Piers uses Smoothwall filtering and monitoring systems to support safeguarding, online safety and information security. The IT Team, in partnership with the Lead DSL and Online Safety Team, is responsible for ensuring that filtering and monitoring arrangements remain effective, proportionate and responsive to emerging risks.

Smoothwall filtering applies to devices connected to the Young Epilepsy/St Piers network, including access by students, staff and visitors. Appropriate technical controls are used to restrict access to illegal, inappropriate and harmful content whilst supporting the safe use of technology.

Content within the following categories is blocked or restricted through the organisation's filtering arrangements:

- Known malicious websites
- Gambling
- Piracy and copyright infringement
- Malware, hacking and cybercrime resources
- Self-harm, eating disorder and suicide-related content
- Pornographic content
- Terrorism, radicalisation and extremist material
- Adult offensive content
- Bullying and harassment
- Drugs and substance misuse
- Unapproved artificial intelligence (AI) platforms

Where staff or students identify a legitimate website or resource that is required for educational, therapeutic or operational purposes but is restricted, a request may be submitted to the IT Team for review

Internet access is managed through a range of user profiles. Students who require personalised access arrangements may be allocated bespoke filtering permissions in accordance with their Online Safety Risk Assessment.

Monitoring alerts are configured for student internet activity and are reviewed in accordance with organisational procedures. Alerts are shared with the Lead DSL and members of the Online Safety Group where safeguarding concerns are identified. All safeguarding concerns relating to internet use must be recorded on MyConcern®.

Where concerns regarding staff conduct are identified through organisational systems or reported by others, these will be brought to the attention of the appropriate senior manager, Human Resources and the Lead DSL for consideration and action in accordance with organisational procedures

The Online Safety Team and Head of IT will undertake regular reviews of filtering and monitoring arrangements and provide assurance regarding their effectiveness

Staff training

All staff will receive online safety training as part of induction and probation and complete annual refresher e-learning.

Training will support staff to understand the benefits and risks associated with internet use, recognise online safety concerns and respond appropriately to safeguard students.

Trustees and Governors will receive regular updates and assurance regarding online safety, filtering and monitoring arrangements, emerging risks and safeguarding themes through governance and reporting processes.

The Safeguarding Team, Online Safety Team and relevant members of the IT Team will maintain up-to-date knowledge of online safety through professional development, training, guidance, legislation updates and best practice resources.

Communications

The organisation's email system is primarily provided to support work-related communications and is subject to appropriate security, monitoring and information governance controls. Limited personal use may be permitted in accordance with the IT Acceptable Use Agreement and associated organisational policies, provided that such use does not interfere with work responsibilities, compromise security, or breach organisational policies. Staff must use their organisational email account for all work-related communications.

Users must report immediately to their manager, the IT Team or a DSL/DSO any communication that is offensive, discriminatory, threatening, bullying, suspicious or causes concern. Such communications should not be responded to and should be retained where required for investigation

All digital communication between staff and students or service users, parents or carers, including email, messaging platforms, blogs or other online tools, must be professional in tone and content and must only take place through approved organisational systems. Personal email accounts, personal messaging services and personal social media accounts must not be used to communicate with students, parents or carers.

Staff must ensure that significant communications relating to students are recorded within the appropriate organisational systems in accordance with record-keeping requirements. Email should not be relied upon as a record management system.

Social Media

Some students at St Piers choose to access social media. Students should only access social media platforms where they meet the minimum age requirements and where this is consistent with their individual needs, capacity and online safety risk assessment

Students should be supported to understand privacy settings, online relationships, digital footprints, safe sharing of information and how to report concerns whilst using social media platforms.

As individuals in positions of trust, staff must not establish personal online relationships with students or interact with them through personal social media accounts. Further guidance is available within the Child and Adult Protection and Safeguarding Procedure and Staff Code of Conduct.

Staff must familiarise themselves with the organisation's Social Media Guidance and act in accordance with it. Staff should recognise that students, former students, parents and carers may be able to access information shared through personal social media accounts. Appropriate privacy settings should therefore be maintained at all times. Staff should carefully consider the content they post online and the potential impact on their professional role and the reputation of the organisation. **Think before you post.**

Staff should be aware that privacy settings cannot guarantee that information shared online will remain private. Content posted online may be copied, shared or accessed by others, regardless of privacy settings. Staff should carefully consider whether any content they post could affect their professional reputation, their position of trust, or the reputation of Young Epilepsy/St Piers. Staff should also be mindful that liking, sharing or commenting on online content may be interpreted as endorsing that content.

Staff must:

- Not refer to students, parents/carers or colleagues on social media.
- Not engage in online discussions about members of the Young Epilepsy/St Piers community.
- Not share content that may compromise their professional standing or the reputation of the organisation.
- Make clear that personal views are their own and do not represent Young Epilepsy/St Piers.
- Review privacy and security settings on personal social media accounts regularly.
- Never use a student's device, account or login credentials for their own purposes.

Personal use of social media that does not reference or impact upon Young Epilepsy/St Piers falls outside the scope of this procedure. However, where personal use affects the organisation, students, colleagues or professional conduct, it may be considered under relevant organisational policies and procedures.

Emerging Technologies

Digital technologies continue to evolve rapidly and may present both opportunities and safeguarding risks for students. Young Epilepsy/St Piers will regularly review emerging technologies, platforms and applications to assess their educational value, accessibility, safeguarding implications and impact on student wellbeing.

Where new technologies, applications or digital platforms are introduced, appropriate risk assessments will be undertaken to ensure that any safeguarding, privacy, information governance and cyber security risks are identified and managed appropriately before implementation

Particular consideration will be given to emerging technologies such as artificial intelligence (AI), virtual reality (VR), livestreaming platforms, social media applications and encrypted messaging services, ensuring that students are supported to access these safely and in accordance with their individual needs and risk assessments.

Photography and Videos

Digital imaging technologies can support learning, communication, social interaction and record keeping. However, staff, students and parents/carers must be aware of the risks associated with creating, storing and sharing images online. Once shared, images may remain accessible indefinitely and could contribute to cyberbullying, grooming, exploitation, image-based abuse or cause distress. Images may also be copied, manipulated or altered, including through the use of artificial intelligence (AI).

Staff should support students and service users to understand the risks associated with taking, sharing and distributing images, and must be familiar with relevant Information Governance guidance relating to photography and video recording.

Photographs and videos must only be taken using a Young Epilepsy/St Piers device. Appropriate consent must always be obtained before taking an image. Where a student has the capacity to provide informed consent, their decision to agree or decline must be respected and recorded.

Images must have a clear professional purpose. Staff must not take photographs or videos that could be inappropriate, intrusive or open to misinterpretation. Photographs of anyone in a state of undress, in underwear or nude must never be taken.

All images must be stored securely and shared only where there is a legitimate professional need. Photographs of students must only be shared using Young Epilepsy/St Piers systems and within the scope of the consent provided. Images must be stored securely on approved organisational systems.

Managers are responsible for ensuring that images are routinely reviewed and removed from devices once they have been securely transferred and are no longer required.

The Therapy Team may take photographs of students as part of spinal clinic assessments. These photographs must be taken using a St Piers device and explicit consent must be obtained and recorded. *Further information can be found within the Therapy Photographing of Injuries Procedure.* Access to such images must be restricted to those with a legitimate professional need. Where images need to be shared with staff teams, there must be a clear rationale and staff must be advised that the images must not be copied, downloaded or distributed further

In exceptional circumstances, the Safeguarding Team or medical professionals may need to photograph injuries or bruising for safeguarding or clinical purposes. Such images must only be taken on an authorised device by an authorised member of staff. Care must be taken to minimise unnecessary exposure, maintain dignity and ensure that images are stored and shared securely. Advice should be sought from the Head of Safeguarding and Quality where required.

Mobile Phones

All staff must read, understand and comply with the Staff Code of Conduct, IT Acceptable Use Agreement and associated organisational policies relating to the use of mobile devices and technology. Staff who use the internet or mobile devices in an inappropriate, unsafe or unlawful manner may be subject to disciplinary action.

Where students have access to mobile phones or other personal devices, staff must support them to use these safely, responsibly and in accordance with their Online Safety Risk Assessment. Students should be encouraged to understand the benefits and risks associated with mobile technology, including privacy, online relationships, information sharing and personal safety.

The Student Agreement provides guidance on the safe and appropriate use of mobile phones and personal devices. Students must not use mobile phones during lessons in school or college unless this forms part of an agreed educational activity or reasonable adjustment. Students are expected to comply with the rules and expectations that apply within the specific service, setting or provision they attend.

Arrangements relating to the possession, storage and use of mobile phones and personal devices may differ between services. Where individual arrangements are required, these should be based on the student's age, needs, capacity, wellbeing and assessed level of risk, and clearly set out when and how access to personal devices is permitted.

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

Support for Parents and Carers

Parents and carers play an important role in helping children and young people to develop safe and responsible online behaviours. Young Epilepsy/St Piers recognises that online safety can be challenging for families, particularly as technology, social media platforms and online risks continue to evolve.

Young Epilepsy/St Piers will provide information, advice and resources to support parents and carers to understand online safety risks and promote safe use of technology at home. This may include:

- Information shared through the curriculum and student learning activities.
- Letters, newsletters, ParentMail communications and the website.
- Awareness campaigns and events, such as Safer Internet Day.
- Signposting to relevant guidance, resources and specialist organisations.

5. Roles and Responsibilities

Trustees

The Trust Board has overall responsibility for safeguarding the children and young adults supported by Young Epilepsy/St Piers, including protecting them from online risks and harm. Trustees will seek assurance that appropriate online safety, filtering and monitoring arrangements are in place, that staff and students receive suitable education and training, and that governors and leaders effectively oversee online safety across the organisation.

Governors

Keeping Children Safe in Education (KCSIE) 2026 states:

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).

The Education Governing Body is responsible for providing strategic oversight and assurance that online safety arrangements are effective across St Piers School, College and Residential Services. This includes seeking assurance that:

- students receive online safety education that is appropriate to their age, abilities, communication needs and vulnerabilities;
- online safety is embedded within the curriculum and residential provision;
- appropriate filtering and monitoring systems are in place and reviewed regularly;
- staff receive suitable online safety training;
- safeguarding concerns relating to online safety are identified, reported and responded to appropriately; and
- leaders monitor the effectiveness of online safety arrangements and take action where improvements are required.

IT Team

The Head of IT is responsible for ensuring that the technical infrastructure at Young Epilepsy/St Piers is secure, resilient and protected against misuse, unauthorised access and cyber-attacks. They are responsible for the day-to-day management of information security, cyber security arrangements and the response to information security incidents.

The IT team will provide and manage access to digital technology and internet services in accordance with organisational procedures, approved risk assessments and guidance from relevant managers. They will also provide reports relating to internet usage, filtering and monitoring where required.

The IT Helpdesk will support students to connect approved personal devices to the Young Epilepsy/St Piers network. Responsibility for the maintenance, security, functionality and condition of personal hardware and software remains with the device owner.

The Head of IT will work in partnership with the Lead DSL and Online Safety Team to ensure filtering and monitoring systems are effective, proportionate and compliant with statutory guidance. This includes carrying out regular reviews of filtering and monitoring arrangements, responding to emerging risks, supporting safeguarding investigations where appropriate, and providing assurance to leaders and governors regarding the effectiveness of these systems

Online Safety Group

St Piers has a multidisciplinary Online Safety Group which meets regularly to oversee, promote and develop good practice in online safety across the organisation. The team works closely with the Lead DSL, Head of IT and operational leaders to ensure that online safety arrangements remain effective, proportionate and responsive to emerging risks.

The Online Safety Group is responsible for:

- Promoting a positive and safe culture in relation to the use of technology and the internet.
- Acting as a source of advice and expertise on online safety matters.
- Monitoring emerging online safety risks, trends, technologies and safeguarding concerns that may affect students.
- Raising awareness and understanding of online safety amongst staff, students, parents and carers.
- Supporting the development, review and implementation of online safety policies, procedures and guidance.
- Supporting the delivery of online safety training and awareness activities.
- Working with the Lead DSL and Head of IT to review the effectiveness of filtering and monitoring arrangements and identify any required improvements.
- Ensuring the organisation remains informed of relevant legislation, statutory guidance and best practice relating to online safety.
- Identifying themes, trends and learning from online safety incidents to support continuous improvement.

Education and Residential Services Senior Management

As leaders responsible for the care, support and education of students, senior managers within education and residential services must ensure that:

- Students are able to access digital technology and the internet in a way that promotes learning, communication, independence and wellbeing, whilst taking account of their individual needs, vulnerabilities and assessed risks.
- Appropriate online safety risk assessments are completed, regularly reviewed and implemented for students where required, ensuring a proportionate balance between safeguarding and access to technology.

- Staff understand and implement agreed online safety controls, risk management strategies and support plans for the students they work with.
- Student access to technology is monitored appropriately and concerns, trends or emerging risks are acted upon without delay.
- Online safety is embedded within educational, therapeutic and residential practice and reflects the needs of learners with special educational needs and disabilities (SEND).
- Staff receive appropriate online safety training and are kept informed of emerging risks, technologies and safeguarding developments.
- Safeguarding concerns relating to online activity are identified, reported and responded to in accordance with safeguarding procedures.
- Arrangements for filtering, monitoring and supervision remain effective within their areas of responsibility and any concerns are escalated to the Lead DSL and Head of IT as appropriate.

Safeguarding Team

The Safeguarding Team provides advice, oversight and leadership in relation to online safety concerns affecting students and supports staff to respond appropriately to emerging risks.

The Safeguarding Team is responsible for:

- Providing advice and support to staff where there are concerns about a student's safety and wellbeing in relation to online activity or technology use
- Responding to reports of online safety concerns and ensuring appropriate safeguarding action is taken where a student may be at risk of harm, exploitation, abuse, cyberbullying, grooming, sextortion, image-based abuse or exposure to harmful online content.
- Working with relevant managers, parents/carers, external agencies and partner organisations where online safety concerns require a multi-agency response.
- Liaising with the Head of IT where concerns require consideration of filtering, monitoring, internet access, cyber security or the review of online activity.
- Ensuring that online safety concerns are recorded, monitored and escalated in accordance with safeguarding procedures.

- Supporting the delivery of online safety awareness, training and safeguarding advice across the organisation.
- Working in partnership with the Head of IT to ensure that filtering and monitoring arrangements remain appropriate, effective and proportionate to the risks faced by students.
- Monitoring themes, trends and emerging risks relating to online safety and using this information to inform safeguarding practice, policy development and service improvement.

All Staff

All staff have a duty of care to the children and young adults supported by Young Epilepsy/St Piers. As part of this responsibility, all staff must:

- Maintain an up-to-date awareness of online safety risks, emerging technologies and the requirements of this Online Safety Procedure.
- Read, understand and comply with the Staff Code of Conduct, IT Acceptable Use Agreement and associated organisational policies.
- Report any concerns regarding a student's safety, wellbeing or online activity to the Safeguarding Team without delay and in accordance with safeguarding procedures.
- Support students to develop safe and responsible online behaviours, in a manner appropriate to their age, understanding, communication needs and vulnerabilities.
- Promote and role model safe, respectful and responsible use of technology and the internet.
- Remain alert to online risks including cyberbullying, grooming, online exploitation, harmful content, fraud, image-based abuse, sextortion, misinformation and risks associated with artificial intelligence.
- Record and report online safety concerns in line with this procedure and the Child and Adult Protection and Safeguarding Procedure.

Tutors/Teachers and Senior House Managers/House Managers

- As the professionals responsible for the day-to-day planning, support and oversight of students, tutors, teachers and Senior House Managers/House Managers must ensure that:

- Staff within their area understand their responsibilities in relation to online safety and receive appropriate guidance, support and training to implement this procedure effectively.
- Online safety risk assessments are completed, regularly reviewed and amended where required to reflect changing needs, vulnerabilities and emerging risks.
- Relevant information from online safety risk assessments is communicated to staff who support the student and, where appropriate, to parents, carers and the student themselves. Any restrictions, controls or changes to internet access should be clearly explained.
- The IT Team is informed where a student's internet access requirements fall outside standard access arrangements or where personalised filtering, monitoring or access controls are required.
- Students are appropriately supervised and supported in their use of technology, taking account of their age, abilities, communication needs, vulnerabilities and assessed risks.
- Any breaches of this procedure, online safety concerns or emerging risks are reported promptly to the appropriate safeguarding and management teams.
- Online safety is embedded within learning opportunities, daily practice, key-working, residential support and other relevant activities to help students develop safe and responsible online behaviours.
- The use of digital technology, mobile devices, social media, photography, video and other online platforms is monitored in accordance with organisational procedures and individual risk assessments

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 provides a guest Wi-Fi network for visitors. Access to the guest Wi-Fi is subject to the organisation's filtering and monitoring arrangements and is intended for lawful and appropriate use only.

All visitors must be informed that internet traffic and network activity may be monitored for safeguarding, security and operational purposes in accordance with the organisation's information governance and data protection arrangements.

Visitors are expected to use the guest Wi-Fi responsibly and in accordance with the organisation's safeguarding, online safety and information security expectations. Any concerns regarding inappropriate use should be reported to a member of staff.

6. Data Protection

Young Epilepsy/St Piers processes, stores, shares and manages personal information in accordance with current data protection legislation, including UK GDPR and the Data Protection Act 2018.

All staff using internet, digital and mobile technologies must comply with the organisation's information governance requirements and associated policies and procedures, including:

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

These documents set out how information should be collected, used, stored, shared and disposed of securely and can be accessed via the intranet.

7. Reporting and Monitoring

If staff become aware of inappropriate, harmful or potentially illegal online content, they must report this immediately to an appropriate member of staff. Where appropriate, the concern should be escalated to the Lead DSL and/or Head of IT, including details of the website or content where possible. All concerns will be recorded and managed in accordance with safeguarding and organisational procedures.

Where there are concerns that a student's or service users' online activity may place them at risk of harm, staff must notify a DSL/DSO without delay. The DSL may work with the IT Team to review relevant online activity and determine whether additional safeguarding measures or support are required.

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

Any material believed to be illegal will be reported to the appropriate agencies, including the Internet Watch Foundation (IWF), the Police, Child Exploitation and Online Protection (CEOP), Children's Social Care or Adult Social Care as appropriate.

This procedure will be reviewed annually and sooner if required in response to changes in legislation, safeguarding guidance, technology, emerging risks or learning from incidents.

8. Procedure for Managing Prohibited and Inappropriate Internet Use

Some online activity is illegal and strictly prohibited within Young Epilepsy/St Piers. This includes, but is not limited to, accessing, creating, possessing or sharing indecent images of children, online grooming, cyberbullying, hate crime, extremist material and other unlawful content

Other online activity may not be illegal but may still be inappropriate, unsafe or harmful depending on the age, needs, capacity and vulnerabilities of the student concerned. Examples are provided in Appendix 2.

Any online safety concerns raised must be reported immediately to a DSL/DSO who will assess the concern and liaise with relevant agencies where appropriate, including:

- The Police, where criminal activity is suspected.
- Children's Social Care.
- Adult Social Care.
- The Local Authority Designated Officer (LADO), where concerns relate to a professional.
- Parents or carers, where appropriate.
- Action Fraud, where fraud, cybercrime or online financial exploitation is suspected.

Where necessary, evidence relating to an online safety concern may need to be preserved. Staff should not delete content, interfere with devices or undertake their own investigations. Advice should be sought from the DSL/DSO and Head of IT to ensure that evidence is retained appropriately.

If staff become aware of suspected indecent images of children, they should avoid viewing, copying, forwarding or saving the material wherever possible. The DSL/DSO must be informed immediately and, where relevant, details such as website addresses or online locations should be recorded.

Any online safety concern involving a student must be recorded on MyConcern® in accordance with safeguarding procedures.

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. Childnet International
6. UK Safer Internet Centre
7. Net Aware
8. BBC Own It
9. Parentzone
10. Kidsmart
11. Mencap- Parent's guide to internet safety
12. Young Minds
13. Childline – 0800 1111
14. Action Fraud
15. The professionals Online Safety Helpline (POSH)
16. Internet Matters
17. NSPCC
18. UKIS – Sharing nudes and semi-nudes: advice for education settings working with children and young people
19. 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 procedure is agreed by the Trust Board and will be implemented by all departments.	
Signed:	**Date:**
Chief Executive  **Jane Beaven, Chief Executive**	**01 September 2026**
Chair of Trustee Board Markus Ruetimann **Chair of Trustee Board:** **Markus Ruetimann**	**01 September 2026**
Date of next review:	**31 August 2027**

Version table			
Creation: - Gill Walters in consultation with Head of IT **Approved by: CEO**			
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
6	11 August 2026	Annual review and update in line with KCSIE 2026 and the Online Safety Act 2023. Expanded guidance relating to AI, sextortion, image-based sexual abuse, VAWG, filtering and monitoring, and SEND-specific online vulnerabilities. FAQs are published on the intranet as a standalone document (previously 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 and young people with special educational needs and disabilities (SEND) may be at increased risk of cyberbullying, online exploitation and other forms of online abuse and may require additional support to stay safe online.

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.

Violence Against Women and Girls (VAWG)

Violence Against Women and Girls (VAWG) can occur online as well as offline. Online forms of abuse may include misogynistic content, sexual harassment, unwanted sexual messages, coercive or controlling behaviour, image-based abuse, stalking, intimidation, threats, and the sharing of sexual images without consent.

Children, young people and adults with vulnerabilities may be at increased risk of being targeted online and may require additional support to recognise abusive behaviour and seek help. Some forms of online abuse may become normalised within social media, gaming platforms, messaging applications and online communities. It is important that staff remain alert to signs that an individual is experiencing online harassment, coercion or exploitation.

Online VAWG may also involve the use of emerging technologies, including artificial intelligence, to create manipulated or synthetic images, videos or audio intended to harass, humiliate, threaten or exploit others.

Any concerns relating to online harassment, misogyny, image-based abuse, coercive behaviour, stalking, sexual exploitation or other forms of VAWG should be treated as safeguarding concerns and responded to in line with the Child and Adult Protection and Safeguarding Procedure. Concerns should be reported to a DSL/DSO at the earliest opportunity.

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.

Children, young people and vulnerable adults may be at greater risk of fraud and cybercrime due to limited awareness of online risks or a reduced ability to recognise scams and manipulation. Those with learning disabilities, communication needs or cognitive vulnerabilities may be particularly susceptible to financial exploitation, coercion and online fraud. It is important that students are supported to recognise these risks and know how to seek help if concerns arise.

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, guidance from the UK Council for Internet Safety (UKCIS) supports a proportionate safeguarding response that avoids unnecessarily criminalising children and young people.

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.

Image-Based Sexual Abuse (including so called 'revenge pornography')

Image-based sexual abuse occurs when intimate or sexual images or videos are created, shared, threatened to be shared, or distributed without a person's consent. This can include images that have been altered, manipulated or generated using artificial intelligence.

Under the Criminal Justice and Courts Act 2015, it is a criminal offence to disclose private sexual photographs or films without consent and with the intention of causing distress. This may occur online or offline, including through social media, messaging applications, email, websites or other digital platforms.

Image-based sexual abuse may occur within current or former relationships, but can also arise through online grooming, coercion, sextortion, exploitation or blackmail by individuals unknown to the victim. Children, young people and vulnerable adults may be at particular risk and should be supported to recognise unsafe online relationships, requests for sexual images, coercive behaviour and attempts to manipulate or exploit them.

Advances in technology, including artificial intelligence, have increased the risk of manipulated, synthetic or 'deepfake' sexual images being created and shared without consent. Such incidents should be treated seriously regardless of whether the images are genuine or artificially generated.

All students should be supported to understand the risks associated with creating, sharing or allowing others to take intimate images or videos of them. Any instance of a student being the victim or perpetrator of image-based sexual abuse, including the non-consensual sharing of intimate images, threats to share images, sextortion or the use of AI-generated sexual imagery, must be treated as a safeguarding concern and reported to a DSL/DSO immediately.

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.

We will treat any suspected grooming as a safeguarding concern and report it to a DSL/DSO immediately

What is AI?

Artificial intelligence (AI) uses computer systems to perform tasks that would normally require human intelligence, such as recognising patterns, generating content, solving problems and making decisions. Generative AI (GenAI) can create text, images, audio and video in response to user prompts. Common tools include:

- Text: ChatGPT, Google Gemini, GrammarlyGO
- Images and Video: DALL·E, Midjourney

AI technology is developing rapidly and can generate highly realistic content. Whilst it can offer educational, communication and accessibility benefits, it may also be used to create harmful, misleading, abusive or illegal content. Some AI-powered applications and chatbots may expose users to misinformation, inappropriate content or harmful influences.

As part of online safety education, students should receive support appropriate to their age, understanding, communication needs and vulnerabilities to recognise that images, videos, audio recordings and information encountered online may not always be genuine. Staff should consider a student's ability to recognise manipulated, synthetic or AI-generated content when completing online safety risk assessments.

AI can exacerbate existing safeguarding risks, including:

- **Misinformation and Scams:** AI-generated content can be used to create convincing phishing emails, fraudulent messages and misinformation.
- **Child Sexual Exploitation and Abuse:** AI may be used to create manipulated or synthetic sexual images, including deepfake imagery involving children.
- **Grooming, Catfishing and Sextortion:** Offenders may use AI-generated profiles, images, audio or messages to deceive, groom or coerce children and vulnerable adults.
- **Image-Based Abuse:** AI can be used to create, alter or distribute intimate images without consent, causing distress and harm to victims.
- **Harmful or Addictive Applications:** Some unmoderated AI tools may encourage harmful behaviours, blur the distinction between reality and fiction, or expose users to inappropriate content.

Emerging Technologies and Online Risks

There are a number of emerging technologies and online risks which staff should be aware of:

Virtual Reality (VR) and Metaverse Safety

These environments present unique safeguarding challenges, including realistic avatars, private virtual spaces, immersive experiences and opportunities for grooming, exploitation or harmful interactions. Staff should be aware of the risks and follow agreed safety protocols before supporting student access.

Live Streaming Risks

Students may use live streaming platforms and services which allow real-time interaction with large audiences. Staff should be aware of the risks associated with inappropriate contact, exploitation, financial coercion, privacy breaches and the sharing of personal information. Appropriate supervision and privacy settings should be considered.

End-to-End Encrypted Messaging Applications

Applications such as WhatsApp, Signal and Telegram may present safeguarding challenges because content cannot routinely be monitored by service providers. Online safety risk assessments should take account of a student's use of encrypted messaging services and any associated vulnerabilities or risks.

AI Use by Staff

Staff should be aware that generative AI tools may produce inaccurate, biased, misleading or unsafe content. Information generated through AI should not be relied upon without appropriate professional review and verification. Staff must ensure that the use of AI does not compromise safeguarding, confidentiality, data protection, record keeping requirements or professional judgement. Personal, sensitive or confidential information must not be entered into public AI systems unless expressly authorised and compliant with organisational policy.

AI and Student Vulnerability

Students should be supported, at a level appropriate to their age, understanding, communication needs and vulnerabilities, to recognise that images, videos, audio and information encountered online may not always be genuine. Staff should consider the impact of AI-generated and manipulated content when assessing online risks and supporting students to use technology safely.

What is Sextortion?

Sextortion is a form of sexual exploitation and blackmail where an offender uses real, manipulated or AI-generated intimate images, videos or information to coerce, threaten or exploit another person. Whilst sextortion is often financially motivated, offenders may also seek further images, sexual acts, personal information or ongoing contact.

Offenders may:

- Pose as peers or trusted adults to establish relationships online and gain a person's trust.
- Groom children, young people or vulnerable adults through social media, gaming platforms, messaging applications or video chat services.
- Coerce individuals into sharing sexual or intimate images or videos.
- Use genuine, stolen, manipulated or AI-generated images to make threats, demand money, obtain further images or exert control over a victim.

Key Safeguarding Actions

- Educate students about online grooming, sextortion, image-based abuse and the risks associated with artificial intelligence.
- Encourage students to report suspicious contacts, threats, coercion or requests for images immediately.

- Ensure online safety risk assessments consider vulnerabilities associated with social media, messaging platforms, gaming platforms and emerging technologies.
- Preserve evidence where appropriate and seek advice from the DSL/DSO/IT Team before taking any action that may compromise an investigation.
- Treat all incidents of sextortion as safeguarding concerns and report them immediately to a DSL/DSO. Referrals to the police, children's social care, adult social care or other agencies should be considered where appropriate

Appendix 2: Overview of the acceptability of online behaviour

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

		Acceptable at specific times[1]	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 discrimination, hatred, misogyny, violence against women and girls (VAWG) or other harmful content.			X	X

[1] The acceptability of some online activities may be determined by a student's age, capacity, vulnerabilities, individual risk assessment and support needs. Activities marked as acceptable for nominated users or at specific times must be subject to appropriate supervision and safeguards.

		Acceptable at specific times[2]	Acceptable for nominated users	Unacceptable	Illegal
	Threatening, abusive, coercive or intimidating behaviour, including online harassment, stalking and image-based abuse.			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	
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	

[2] The acceptability of some online activities may be determined by a student's age, capacity, vulnerabilities, individual risk assessment and support needs. Activities marked as acceptable for nominated users or at specific times must be subject to appropriate supervision and safeguards.

	Acceptable at specific times[3]	Acceptable for nominated users	Unacceptable	Illegal
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			
Creating, sharing or possessing AI-generated intimate images of another person without consent				X
Entering personal, confidential or sensitive information into public AI systems			X	

[3] The acceptability of some online activities may be determined by a student's age, capacity, vulnerabilities, individual risk assessment and support needs. Activities marked as acceptable for nominated users or at specific times must be subject to appropriate supervision and safeguards.