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.

The subject of online safety continues to grow exponentially due to the ever increasing and emerging technologies and requires us to adopt an approach of enquiry, transparency, partnership and common sense.

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. Risks and Benefits

Digital technologies offer us all abundant opportunities to learn and develop, communicate, be creative and be entertained. The advantages of the internet can and should out-weigh the disadvantages.

For children and young adults with a disability, the value of using mobile devices and the internet can be even greater than for their non-disabled peers. The use of assistive technologies can aid communication and social networking to help children and young adults with a disability who are isolated, to connect to others. Disabled people can also access opportunities and services that they may be isolated from, such as online shopping and banking. Therefore, as professionals working with children and young adults with a disability, we must be proactive in seeking these opportunities.

Due to the rapid advancement of digital technologies, children and young people embrace and understand advancement in the internet and mobile telephones as the 'norm', and often view this 'virtual world' as an extension to their physical world. However, this can create some risk to children and vulnerable adults that we must be aware of, and as far as possible help them to understand and avoid. Some of the dangers the virtual world can pose to children / adults at risk include:

- Attendance and attainment at school and college can be affected by 'vamping'- lack of sleep due to using technology.
- Being 'groomed' online by others (often pretending to be other young people) with the ultimate aim of exploiting them sexually.
- Being bullied or 'trolled' by others via social networking sites, websites, instant messaging and text messages; this is often known as 'cyber-bullying'. Due to people having more or less 24 hr access to mobile technologies and the internet, such issues can be all encompassing and concerning.
- Inappropriate (i.e., threatening or indecent) images of children and young people being taken, uploaded and circulated via social network websites, mobile telephones and video broadcasting websites such as YouTube, often by other young people. This can lead to bullying, blackmail or exploitation.
- The dangers attached to gang culture can rapidly accelerate online as gangs 'advertise' or promote themselves via websites or social networking sites or if threats of violence, threats to an individual's life or threats of retaliation are posted online by opposing gang members.
- Unsuitable websites, content and images can easily be accessed online (e.g., ignoring age ratings in games enabling exposure to violence, explicit and extreme content; pornography; lifestyle websites such as pro-anorexia, self-harm, suicide or hate sites).
- Being recruited by people with extreme political and cultural views, which can lead to their radicalisation.
- Becoming the victims of fraud because of sharing personal information.

The breadth of issues classified within online safety is considerable but can be categorised into four areas of risk; **Content, Contact, Conduct and Commerce**.

Content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-semitism, radicalisation and extremism.

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.

Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g., consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.

Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you we feel that any pupils, students or staff are at risk, we need to report it to the Anti-Phishing Working Group.

These areas are covered within Young Epilepsy/St Piers' Online Safety training, which is reviewed as appropriate, in line with legislative changes and at least annually.

Ignoring these dangers can lead to serious gaps in our responsibilities towards safeguarding children and adults at risk.

Some of the common technologies being used include the following:

- The Internet
- Artificial Intelligence
- Email
- Instant messaging
- Blogs / Vlogs
- Podcasts
- Web cameras
- Social networking sites such as Facebook, Twitter and Instagram
- Location based social networking
- Video broadcasting sites such as YouTube
- Chat rooms and forums
- Skype
- Zoom
- WhatsApp
- Snapchat
- Instagram
- Online gaming rooms and platforms

- Music download sites
- Mobile phones with camera and video functionality
- 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 children and young adults to be wise to these and subsequently to avoid them.

3. National Legislation and Guidance

This procedure links to and harmonises with the following key legislation and national guidance:

- Keeping children safe in education - GOV.UK (www.gov.uk) 2024
- Teaching online safety in schools 2019 (DfE guidance)
- Working together to safeguard children - GOV.UK
- Digital Economy Act 2017
- Criminal Justice and Courts Act 2015
- Serious Crime Act 2015
- Defamation Act 2013
- Education Act 2011
- The Equality Act 2010
- Education and Inspection Act 2006
- Communications Act 2003
- Sexual Offences Act 2003
- Regulation of Investigatory Power Act 2000
- Data Protection Act 1998
- The Human Rights Act 1998
- Protection from Harassment Act 1997
- The Computer Misuse Act 1990
- Malicious Communication Act 1988

4. Implementation of Procedures

Online safety is not just about recognising the risks that exist for children and adults at risk accessing the internet and mobile devices, but it is about putting in place interventions to reduce the level of risk.

St Piers 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 should have an Online Safety Risk Assessment in place regarding their access to the internet and use of technology, and this must be reviewed at least annually. The risk assessment must be personalised for each student, thinking of their specific needs and the risks posed to them.

These assessments should be shared with relevant persons, including where appropriate the young person and their parents to ensure clarity and a unified approach. These risk assessments must balance risk against benefit and not unnecessarily restrict a student's access to digital technology.

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.

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:

12. Students under the age of 18 years
13. Students over the age of 18 years with capacity
14. Students over the age of 18 years without capacity
15. Staff
16. Visitors
17. Staff who live on campus
18. 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.

Where concerns are raised through this, regarding staff or student 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

The development of digital imaging technologies has created significant benefits to learning, maintaining relationships with others and social interaction. However, staff, parents / carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

- When using digital images, staff must inform and educate students about the risks associated with taking, using, sharing and distributing images. Staff should read the Information Governance guidance related to photography.
- Staff must only use a Young Epilepsy/St Piers device when taking a photograph or video of a student.

- Staff must ensure that the necessary consent is in place and that if a student has capacity to agree to a photograph / video, their consent has been given. Where consent is given or declined, this should be recorded.
- Staff must ensure that where photos are taken of students on a Young Epilepsy/St Piers device, these photographs are for a clear purpose and that there are no inappropriate photos of students, or photographs that could be misinterpreted as inappropriate.
- Staff should never take photographs on any device of a student in a state of undress, in their underwear or nude. The only exception to this is where a photograph is taken of a student in a swimming / hydro pool where there is a clear professional justification of the image and their dignity and privacy should never be compromised.
- Staff must also take caution with saving and distributing photographs. Photographs of students must only be emailed from a Young Epilepsy/St Piers email account and with a clear explanation for why the photographs are being distributed, and this must remain within the remit of the consent given. The photographs or videos must be stored securely on the Young Epilepsy/St Piers network.
- Managers are expected to have systems in place to check and delete photographs on any device 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 Safeguarding or medical teams. 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, which outlines the guidance for personal mobile phone use.

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.

Appropriate Use

Within the student contract there is clarification about the expectations and responsibilities of students when accessing the internet. This information is also conveyed to parents / carers of students when their son / daughter commences their placement at St Piers.

The expectations and responsibilities of staff's use of the internet and devices is incorporated into the Code of Condu(alongside IT policies and procedures) which **all staff** must sign when they commence employment (inclusive of agency staff) or volunteer with us. 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.

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 2024 states (126):

Governing bodies and proprietors should ensure that, as part of the requirement for staff to undergo regular updated safeguarding training, including in relation to online safety and for children to be taught about safeguarding, including in relation to online safety, that safeguarding training for staff, including online safety training, is integrated, aligned and considered as part of the whole school or college safeguarding approach and wider staff training and curriculum planning.

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.

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 where 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.

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 Unsuitable/Inappropriate Online Activity

Some internet activity e.g., accessing child abuse images, cyber bullying etc. or distributing racist material is illegal and is banned at Young Epilepsy/St Piers.

There are however a range of activities that may, generally, be legal but would/may be inappropriate at Young Epilepsy/St Piers, dependent on student ability/capacity. **See Appendix 3**.

Any online safety concerns from staff, students, volunteers or parents must be passed to the DSL immediately. The DSL will then liaise with external agencies where necessary:

- The police – where illegal activity is involved (e.g., indecent images of children or adult material that breaches legislation)
- Children's Social Care – where a referral needs to be made due to a child's vulnerability
- Adult's Social Care – where a referral needs to be made due to an adult's vulnerability
- 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.

Evidence related to the concerns may need to be secured and so equipment may need to be taken temporarily for this purpose upon advice from the Head of IT.

In cases of staff discovering indecent images of children may have been taken, produced or received, it is important that staff keep themselves safe from viewing such content. Staff must avoid looking at any such content wherever possible and should not attempt to copy the imagery in any way. Staff must alert the DSL as soon as possible. If the images have been accessed via a website, staff should note the URL.

Any concerns regarding online safety involving students, will be recorded on our online safeguarding reporting system.

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

This policy is agreed by the Executive and will be implemented by all departments.	
Signed:	**Date:** .
Position: **Executive Principal**	**Reviewed 31 August 2024** **Next review 01 September 2025**

Version table			
Creation: - Gill Walters **Approved by: - Simone Hopkins**			
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

Appendix 1- Types of Online Risks

Cyber Bullying

It is essential that young people, professionals, parents / carers understand how cyber bullying differs from other forms of bullying, how this can affect young people and what can be done to combat this form of abuse. Cyber bullying is just as harmful as bullying in the 'real' world and clear procedures should be in place to support the victim as well as respond to and manage the perpetrators actions. Young Epilepsy/St Piers has Anti Bullying Guidelines, which provide more information about this.

It must be understood that as cyber bullying can happen 24 hours a day, 7 days a week, 365 days a year and at any time of the day or night, it differs from 'real world' bullying as the victims cannot escape or find respite as it invades places that would ordinarily be safe and private spaces. This also means it is more likely than 'real world' bullying to go unseen.

According to research on cyberbullying in the UK (2009), one third of 11-16 year olds had been targeted, threatened or humiliated online, with the highest rates reported amongst 9-12 year olds. Children with special educational needs were sadly 16 times more likely to be the subjects of persistent bullying,

Those who participate in online bullying often use groups of friends to target their victims. An action as innocent as adding derogatory comments to another person's photograph could rapidly spiral out of control and young people may not realise that their actions constitute bullying. The following are the most commonly reported ways in which bullying occurs:

- Email – Can be sent directly to an individual or group of people to encourage them to participate in the bullying and can include derogatory comments or harassment or examples of homophobia, racism, sexism or other forms of prejudice by either message or image. Something originally meant to be a joke can soon escalate out of control.
- Instant Messaging / Chat Rooms – Messages can be sent directly to an individual or group of people who can then be included in the conversation. Again, conversations can easily escalate out of control. People are not always who they say they are and can approach children and young people with the intention of grooming them. Children and young people may be asked to send inappropriate or explicit photos of himself or herself to someone who they are unaware is an abuser.
- Social networking sites – Anonymous profiles can be set up on social networking sites to make fun of someone and each person contributing to these pages can soon worsen the problem. Inappropriate and threatening comments and images can also be posted and circulated about individuals without their consent. People are not always who they say they are on social networking sites and can approach children and young people with the attention of grooming them.
- Mobile phone – Anonymous and abusive or age inappropriate text or video messages, photograph messages and phone calls can be shared via mobile phones. This also includes the sharing of videos of physical and sexual attacks (which is a criminal offence) on individuals. Many mobile phones have access to the internet and so this creates a risk of accessing inappropriate or harmful content, and many people download applications to their mobile phone, which can mean sensitive information is shared and people can often spend money unknowingly.

- Interactive gaming – Games consoles allow players to chat online with anyone they find themselves matched with in a multi-player game. Sometimes cyber bullies abuse other players and use threats Children and young people can also be groomed via gaming. They can also lock victims out of games, spread false rumours about someone or hack into someone's account.
- Sending viruses – Viruses or hacking programs can be sent by one person to another to destroy their computers or delete personal information from their hard drive.
- Abusing personal information – Personal and sensitive information (including videos and photographs) could be uploaded onto the internet without the victim's permission.
- Social networking sites such as Facebook make it very simple for other users to obtain personal information and photographs of others. They can also get hold of someone else's messaging accounts and chat to people pretending to be the victim.

Although cyber bullying itself can not physically hurt a person, it can leave a young person mentally vulnerable, frightened and lonely and seemingly very difficult to escape from, particularly when this occurs in their own home and can lead to the bullied victim causing harm to themselves, which in some cases may lead to suicide.

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.

Trolling

Trolling is recognised as deliberately inflicting hatred, bigotry, racism, misogyny, or just simple bickering between others. People who partake in 'trolling' are referred to as 'trolls'. They use any environment where they are allowed to make public comments, such as blog sites, social networks (like Facebook® and Twitter®), news sites, discussion forums, and game chat.

Trolling and cyberbullying are sometimes used to mean the same thing, but they are a little different. Cyberbullies target someone and repeatedly attack them, while trolls set out to annoy whoever they can. Trolls want to provoke a reaction or response and it is often not a personal attack because they do not care who their victim is.

People engaging in Internet trolling are immediately committing an offence under the Malicious Communications Act, however the difficulty is in identifying the troll.

People can protect themselves against trolling by:

- Ignoring the troll. Do not respond to nasty, immature or offensive comments -giving trolls the attention they want only gives them more power.
- Blocking the troll. Take away their power by blocking them and if they pop up under a different name, block them again.
- Reporting trolls to website administrators and if they appear again under a different name, report them again.

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.

Indecent images of children

Adults take the majority of indecent images of children (under 18 year olds) that exist. The adult taking the image, has to some degree been party to abusing that child.

Sometimes, children and young people take images or videos of themselves. Youth produced sexual imagery includes:

- A person under the age of 18 creating and sharing an image of themselves to a peer under the age of 18.
- A person under the age of 18 sharing a sexual image created by another person under the age of 18 or an adult
- A person under the age of 18 being in possession of sexual imagery created by someone under the age of 18.

Young people sometimes create sexual imagery of themselves due to taking risks and pushing boundaries as they become more sexually and socially aware and often, through peer pressure. With the prevalence of smart phones with cameras and internet access and the use of Bluetooth technology, images can be shared quickly and easily before young people have the opportunity to consider their actions and the consequences of these.

Sharing images in this way is colloquially known by the term 'sexting' and it can have extremely damaging effects. In the US, a number of young people have committed suicide after images taken of them by previous partners were posted on social networking sites. It is also estimated in a recent Internet Watch Foundation study that 88% of self-taken youth produced sexual images, had been taken from their original location and uploaded elsewhere. An image on the internet has no natural lifespan; once posted an image may be copied by many others including those who may be predatory abusers and will have permanence on the internet.

It can be difficult to distinguish between youth produced sexual imagery resulting from grooming or facilitation by adult offenders who have a sexual interest in children, from the images that result from children and young people simply pushing boundaries and experimenting with their friends.

Crimes involving child abuse images fall under Section 1 of the Protection of Children Act 1978, as amended by section 45 of the Sexual Offences Act 2003 to extend the definition of children from under 16s to under 18s. It is a crime to take, make, permit to take, distribute, show, possess, possess with intent to distribute, or to advertise indecent photographs or pseudo-photographs of any person below the age of 18. Therefore, youth produced sexual imagery is also illegal, however guidance from the UK Council for Child Internet Safety offers guidance on how to handle such situations in a proportionate way, without criminalising children.

It is important that a safeguarding approach is taken when youth produced sexual imagery is found. This means that we will treat the matter as any other safeguarding concern and will speak to Surrey Children's or Adult's Services to make a referral so that the issue can be dealt with at an early stage. The police may need to be involved if a crime is suspected to have taken place. It is important that where it is recognised that students have produced, sent or been sent indecent images of children, that support and education is provided to all the children involved.

'Revenge Pornography'

The Criminal Justice and Courts Act (2015) criminalised so-called revenge pornography. This is defined as "disclosing private sexual photographs and films with intent to cause distress" (CJCA 2015 s33 (1)). The offence applies both online and offline and to images which are shared electronically or in a more traditional way so includes the uploading of images on the internet, sharing by text and e-mail, or showing someone a physical or electronic image.

Although traditionally revenge pornography is identified as something that occurs by two people that are in or have been in a physical relationship, it should also be recognised that sometimes this is happening through the virtual world where people are groomed by strangers who then coerce or blackmail the individual in to providing self-taken sexual imagery. Young people need to be supported to recognise the risks of being approached by strangers on social media and through phishing emails, and to understand what they should do and how they should act if this happens.

It is also important that all young people understand the risks of someone taking an indecent photograph or video of them, regardless of their age, and that they are supported to make an informed decision about whether to allow this to happen. If staff become aware that a student has been the victim or perpetrator of 'revenge pornography', this must be reported as a safeguarding concern.

Grooming

Grooming is defined as 'a process by which a person prepares a child, significant adults and the environment for the abuse of this child. Specific goals include gaining access to the child, gaining the child's compliance and maintaining the child's secrecy to avoid disclosure'.

It is well documented that perpetrators of abuse will attempt to contact children or adults at risk using the internet. In this way, the perpetrator's contact is faceless. They can pretend to be anyone they want to be to attract the child's attention and interaction, and after doing so will use this trust to try and sexually abuse or exploit the child.

One of the issues is that when children and young people communicate via the internet, they are less inhibited and will often share a lot more information than they would when meeting someone face to face.

The Serious Crime Act (2015) introduced an offence of 'sexual communication with a child'. This applies to any adult who communicates with a child where the communication is sexual or where it intends to elicit a sexual response from the child and whereby the adult believes the child to be under 16 years of age. The Act also amended the Sex Offences Act (2003) so it is now illegal for an adult to arrange to meet with someone under 16 years old having communicated with them on one occasion or more.

Artificial Intelligence Risks and 'Sextortion'

What is AI?

Artificial intelligence (AI) is the use of computer systems to solve problems and make decisions. It's already a part of everyday life – you've probably come across it in the form of personalised suggestions on social media, shopping sites or route-planning apps.

Generative AI takes a written prompt and runs it through an algorithm to generate new, 'natural'-seeming content. Tools include:

- Chatbots such as ChatGPT, Google Gemini and GrammarlyGO, which generate text
- Text-to-image programs like DALL-E and Midjourney, which create images

AI technology is developing rapidly, and these tools will only become more sophisticated over time. For example, they'll be able to create more convincing images or videos.

How does AI pose a safeguarding risk?

Rather than being its own safeguarding issue, AI can impact other safeguarding issues:

- **Hacking and scams** – text generation tools can write convincing emails and text messages to trick pupils into giving malicious actors access to their accounts
- **AI-generated child sexual abuse images** – some text-to-image tools could be used to create child sexual exploitation material for sexual gratification or as a means of bullying another pupil
- **'Deepfake' pornography** – super-imposing a person's face into pornographic videos for sexual gratification or to humiliate the person being put in the images. AI technology is used to alter the person's facial expressions to make the video look more convincing
- **'Catfishing' and sextortion** – criminals can use AI-generated profile pictures to appear younger than they are to befriend and groom children and young people, and then solicit information and/or images from them (e.g. nude or semi-nude photos)
- **Fake news and misinformation** – text-to-image tools can be used to create convincing fake photos of world events, which could be used to promote certain beliefs (including hateful ones)

What is sextortion?

Financially motivated sexual extortion (often referred to as 'sextortion') is a type of online blackmail. An adult (or group of adults) threatens to release nude or semi-nude images of a child unless they pay money or do something else to benefit them.

Sextortion is often carried out by offenders in an organised crime group overseas and is motivated by profit.

Sometimes adults pose as children to make contact. They might:

- Groom or coerce the child into sending nudes or semi-nudes and financially blackmail them
- Use images that have been stolen from the child, taken through hacking their account
- Use digitally manipulated images, including AI-generated images, of the child

Appendix 2: Frequently Asked Questions

Q1a. Is it OK for me to add students as friends on social networking sites?

A1a. No. The information available on these sites can blur the professional boundaries and lead to inappropriate relationships or boundaries being formed. This also applies to former students. Any staff member found to be in breach of this guidance will be subject to a disciplinary hearing. Staff should ensure that their security settings on social networking sites protect their information from being accessed by students or former students.

If a student/s is using social networking as part of their curriculum then staff should support them through separate and approved accounts that are set up for this purpose.

Q1b. Is it OK for me to add students' parents as friends on social networking sites?

A1a. No. As above, the information available on these sites can blur the professional boundaries with parents and lead to inappropriate relationships and boundaries being formed. If a staff member already has a personal relationship with a student's parents before joining, then the staff member should disclose this to their manager so that they are aware.

Q2. Can I use my personal mobile phone or camera to photograph or video students I work with?

A2. No. Any photographic or video images should always be recorded and stored on equipment belonging to the organisation and only used for the purposes that written consent has been given for.

Q3. I am concerned regarding a colleague's comments/ behaviour on social media. What should I do?

A3. If the comments have been made whilst your colleague was at work or if the comments refer to work, you should speak to your line manager in the first instance. Please also refer to Young Epilepsy/St Piers' Child and Adult Protection and Safeguarding Procedures and Whistleblowing and Confidential Disclosures Procedures.

Q4. Can I connect my own personal device to the Wi-Fi network at work?

A4. Yes, you can. However, staff are expected to use this in a responsible manner. The IT department monitors its use and misuse or failure to adhere to ***Acceptable Use Guidelines*** may result in access being suspended/ removed.

Q5. I have received an email from an unknown source. What should I do?

A5. If the email is not from a Young Epilepsy/St Piers email address or not from someone you have shared your email address with then it is best to assume that the email is potentially harmful or malicious. Our security filter notices most SPAM or malicious emails, however, on occasion some may get through. If you have any concerns, it is safest just to delete the email.

Q6. Should a student over 18 have access to explicit adult content?

A6. Sometimes - it depends on the individual student. Accessing pornography is legal from the age of 18. However, it is recognised that for some young adults with a lesser developmental age to their chronological age, this may be harmful.

It is important that students are appropriately educated in safe navigation of the internet and this may include access to adult content. Students who have access to this, should have appropriate education on the topic and understand that this may be offensive to some people, therefore should be accessing this in private. Illegal material will never be permitted (see below for a description of this).

Q7. Can I take Young Epilepsy/ St Piers equipment home (e.g., tablet, laptop, and phone)?

A7. If you have permission to take equipment home from the necessary manager, you must ensure you have absolute control over how this is accessed at home. Things that can go wrong include:

parents/guardians/carers accessing the technology inappropriately

Access of adult material- this is never acceptable

Access by others resulting in confidential information about Young Epilepsy/St Piers, its services or students being inappropriately disclosed.

Staff must remember that they will be culpable if an online safety incident occurred so staff must take all necessary precautions to prevent this.

Q8. What is inappropriate material?

A8. Inappropriate is a term that can mean different things to different people. It is important to differentiate between 'inappropriate and illegal' and 'inappropriate but legal'. All staff should be aware that in the former case investigation may lead to criminal investigation, prosecution, dismissal and barring. In the latter, it can still lead to disciplinary action, dismissal and barring even if there is no criminal prosecution.

Illegal

Possessing or distributing indecent images of a person under 18 – and viewing such images on-line may well constitute possession, even if not saved. The police have a grading system for different types of indecent image. Remember that children are harmed and coerced into posing for such images and are therefore victims of child sexual abuse.

Images that depict the following are also illegal:

- bestiality (sexual activities with animals)
- necrophilia (sexual activity with dead people)
- acts which threaten a person's life
- acts which result in or are likely to result in serious injury to a person's anus, breasts or genitals.

Hate/Harm/Harassment

General: There is a range of offences to do with inciting hatred based on race, religion, sexual orientation etc.

Individual: There are particular offences to do with harassing or threatening individuals – this includes cyberbullying by mobile phone, social networking sites etc. It is an offence to send indecent, offensive or threatening messages with the purpose of causing the recipient distress or anxiety.

Inappropriate

Think about this in respect of professionalism and being a role model. The scope here is enormous but bear in mind that actions outside of the workplace that could be so serious as to fundamentally breach the trust and confidence placed in the employee may constitute gross misconduct.

Examples include:

- Posting offensive or insulting comments about the organisation on Facebook.
- Accessing adult pornography on Young Epilepsy/St Piers computers during break.
- Making derogatory comments about students or colleagues on social networking sites.
- Contacting students by email or social networking without senior manager approval.

Q9. What is sexting?

A9. Sexting is the exchange of self-generated, sexually explicit images and messages, through mobile device cameras and webcams using apps or video streaming services.

Many young people refer to it as:

- Dirty pics
- Rude dares
- Nude selfies or sending nudes
- Cybersex.

'Sexting' does not include the sharing of sexual photos and videos of under-18 year olds with or by adults. This is a form of **child sexual abuse** and must be referred to the police.

Anyone who has or sends indecent images of someone **under the age of 18 is breaking** the law.

Both having and distributing images of this nature is an offence under the Sexual Offences Act 2003.

Encouraging someone to take or send 'sexts' can also be illegal

Q10 How can I use ICT appropriately to communicate with Students?

A10. Staff should not use their personal emails or phone numbers to communicate with children. Staff should use Young Epilepsy/St Piers technology for this purpose and ensure the tone is professional and cannot be misinterpreted.

Q11 What signs might be an indicator of concern regarding students?

A11. If a student is facing a safeguarding issue online, they might:

- Spend more time online, or more time offline. This might be reported by their parents or witnessed by staff
- Complain of being tired because they were online all night, or have their phone going off a lot

- Have stronger emotional responses or outbursts to being online – e.g. they may get unusually angry, upset or distant after checking their phone or using their computer/tablet
- Be secretive about their use of the internet or a device – they may refuse to hand their phone in if it's part of school policy, or refuse to tell you what they get up to online
- If a child tells you that they use their device unsupervised – e.g. they play on their iPad when they go to bed – this could be a red flag.

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			