Online Safety Procedure

This procedure implements the Online Safety Policy and aims to ensure Young Epilepsy supports students to access the internet safely, prevent harm being caused to them online and respond to online safety concerns appropriately and sensitively. As is the case with all safeguarding concerns, online safety is the responsibility of all staff.

CONTENTS

1. PURPOSE & 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.

Young Epilepsy knows 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 learners and staff are protected from potential harm online. We will empower our learners 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 Young Epilepsy's 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 Young Epilepsy
- 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.

This procedure applies to all access to the internet and use of technology, including mobile technology, or where learners, staff or other individuals have been provided with setting issued devices for use, both on and off-site.

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.

This procedure applies to all members of Young Epilepsy (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 children and young adults abundant opportunities to learn and develop, communicate, be creative and be entertained. The advantages of the internet can and should out-weigh the disadvantages. The use of digital technologies is now so prevalent and important in society, that we must support students to have access and reap the benefits of this.

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. For example, 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 You Tube, 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; life style 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 three areas of risk; **Content, Contact and Conduct**.

Content - being exposed to illegal, in appropriate or harmful material; for example pornography, fake news, racist or radical and extremist views.
Contact – being subjected to harmful online interaction with other users; for example, commercial advertising as well as adults posing as children or young people
Conduct – personal online behaviour that increases the likelihood of, or causes, harm for example making, sending and receiving explicit images, or online bullying.

These areas are covered within Young Epilepsy's Online Safety training.

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
- 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
- WhatsApp
- 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 2019 (with specific reference to Annex C)
- Teaching online safety in schools 2019 (DfE guidance)
- Working Together to Safeguard Children 2018
- 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.

Young Epilepsy will take all reasonable 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. Young Epilepsy 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 Young Epilepsy 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 beset up to access the internet via the IT Services Department. Access to the internet through any personal devices but using the Charity's WIFI is also filtered and monitored through a separate network system. However access to the internet through 3G and 4G 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 in to 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 Services Department 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 child and adult at risk will have an Online Safety Risk Assessment (see Appendix 3) 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.

It is likely that the risks associated with using mobile technology and accessing the internet for a student, are the same within their education services as they are within their residential environment. Therefore, it is the responsibility of the Teacher / Tutor and the House Manager to work together to complete this assessment. 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 waking curriculum

One of the most important areas for staff at Young Epilepsy is teaching children and adults at risk about how to be digitally resilient.

Online safety is taught to all learners 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. It is imperative that we teach students about acceptable and safe use of technology in order for them to experience the multitude of benefits from using such technology but remain safe whilst doing so.

It is just as important, that similar to all other learning, Online Safety is embedded within the home context by residential support staff. Children and young adults should be supported through every day 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). If staff have any queries about how to deliver online safety support to the students they support, they should contact the IT team, Teacher/Tutor, their manager or the Safeguarding Team.

However, alongside the formal risk assessment(s) and processes, staff must be aware of their role in 'loco parentis' and be mindful of the content children and young people may be exposed to when online and take appropriate action as any 'good' parent would.

Web Content Filtering

The organisation subscribes to Smoothwall, which applies filtering, monitoring and firewall solutions to the wifi. This applies to all access to Young Epilepsy wifi by students, staff and visitors.

Content in the following categories is blocked on our corporate network:

- Known malicious sites
- Gambling
- Piracy and copyright theft
- Malware/hacking
- Pro-self harm, eating disorder or suicide content
- Insecure shopping sites
- Pornography
- Terrorism and violence
- Adult offensive content
- Bullying
- 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.

If staff plan to use a website as part of a lesson or presentation, they should check in advance to ensure that the site is not filtered. The IT Helpdesk is not always able to respond to unblock requests at short notice and can therefore not guarantee that a site will be available when needed.

If any staff discover unfiltered content that they deem to be unsafe, malicious, or offensive they should report this to the IT Helpdesk so that this can be added to our web filter.

Access to the web is via user groups as follows:

1. Students under the age of 18 years
2. Students over the age of 18 years with capacity

3. Students over the age of 18 years without capacity
4. Staff
5. Visitors

.

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 student's Online Safety Risk Assessment must then be reviewed when any changes are made.

The organisation will take reasonable measures to prevent access to inappropriate materials. However, due to the global nature of the internet and its content, it is not always possible to guarantee that such material will never appear on any computer. In the event that such materials are accessed, these must be reported to the IT department so that these sites may be added to the filtered list. Certain sites and programmes are deemed as prohibited (due to being illegal) and will not be available to any user.

Web Monitoring

The Young Epilepsy IT Team are responsible for the operation of Smoothwall and its monitoring of web access by all user groups. Where concerns are raised through this, these are immediately brought to the attention of the Lead DSL and appropriate Director, and they are then managed under the Young Epilepsy disciplinary procedure.

Staff training

At Young Epilepsy, we ensure that all staff working with students are trained in understanding online safety 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 their safeguarding training.

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 Young Epilepsy email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the Young Epilepsy email service to communicate with others when on site or on remote access systems. Staff are reminded however that the use of their Young Epilepsy email should be 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) Young Epilepsy systems. Staff's personal email addresses, text messaging or social media must not be used for these communications.

Students must be taught about online safety issues, such as the risks attached to the sharing of personal details. They are taught strategies to deal with inappropriate communications and reminded of the need to communicate appropriately when using digital technologies.

Social Media

Some students at Young Epilepsy 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 Child and Adult Protection and Safeguarding Procedures and Safe Working Practice Agreement.

Staff are required to familiarise themselves with Young Epilepsy's Social Media Guidance and act within this.

Staff should also ensure that:

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

Staff personal use:

- Personal communications are those made via a personal social media accounts. 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 the Charity 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

Emerging technologies are examined for their benefits and where appropriate, a risk assessment will be formulated before its use is permitted. 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.

Young Epilepsy staff will inform and educate students, parents and staff about these risks and will implement policies to reduce the likelihood of the potential for harm.

- 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 device when taking a photo 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 photo / 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 device, these photos are for a clear purpose and that there are no inappropriate photos of students, or photos that could be misinterpreted as inappropriate.
- Staff should never take photos on any device of a student in a state of undress, in their underwear or nude. The only exception to this is where a photo is taken of a student in a swimming / hydro pool where there is a clear professional justification of the image.
- Staff must also take caution with saving and distributing photos. Photos of students must only be emailed from a Young Epilepsy email account and with a clear explanation for why the photos are being distributed, and this must remain within the remit of the consent given. The photos or videos must be stored securely on the Young Epilepsy network.
- Managers are expected to have systems in place to check and delete photos on any device at least weekly.

The physiotherapy team take photos of students in their spinal clinic. These photos are taken with a Young Epilepsy device and explicit consent is always gained and recorded for these purposes. Please see the Therapy Photographing of Injuries Procedure for further information. These photos 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 photos taken are stored safely and only the necessary therapists have access to these photos. If the photos 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 photos is and that the images must under no circumstances be distributed further.

The Safeguarding Team or Medical Professionals at Young Epilepsy may, in exceptional circumstances, be required to take photos of injuries or bruising on students. Such photos must only be taken on a Young Epilepsy devise and by someone within the Safeguarding or Medical Teams and 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 Safeguarding Manager in such instances.

Mobile Phones

At Young Epilepsy, staff must agree to and sign the Safe Working Practice Agreement, 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 should not use mobile phones whilst in lessons at school or college. Like in any other family setting, within our role of loco parentis there may also be occasions when there are agreed deadlines set for students to use their phones and any other personal mobile devices. For example, it may be agreed that a student switches off their phone at 10pm if their mobile phone use is deemed to be having a negative impact on their attendance at school or college or an impact on their mood.

See Young Epilepsy's 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 and Young Epilepsy's devices. This information is also conveyed to parents / carers of students when their son / daughter commences their placement at Young Epilepsy.

The expectations and responsibilities of staff's use of the internet and devices is incorporated in to the Safe Working Practice Agreement (alongside IT Policies and Procedures) which all staff must sign when they join Young Epilepsy. 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.

Any access to material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, the police and/or CEOP.

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.

Young Epilepsy will therefore seek to 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 (see appendix for further links / resources)

5. ROLES AND RESPONSIBILITIES

All Staff

All Young Epilepsy staff have a duty of care to all of 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 Safe Working Practice Agreement 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 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

Online Safety Coordinators in school and college

There is an online safety coordinator in St Piers School and in St Piers College who is responsible for:

- Developing a safe culture within the school with regards to use of technology
- Being the main point of contact on issues relating to online safety in the school
- Raising awareness and understanding of online safety issues amongst staff and parents and carers
- Keeping up with relevant online safety legislation
- Supporting the safeguarding team to update policies, procedures and 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

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's Information Technology Policies and governance, and for re-issuing them each year following their approval by the Executive.

IT Team

The Network Manager ensures that the technical infrastructure at Young Epilepsy is not open to misuse or attack and that the organisation is compliant with online technical requirements. They also have responsibility for the commissioning, implementation and day-to-day operations of the filtering system in place and works with the Safeguarding Manager to monitor online activity.

The Information Systems Manager is responsible for the day-to-day management of information security activities and responding to Information Security Incidents.

The IT Services Department will provide access to ICT facilities for all students based on the outcome of the risk assessment and 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's systems; they cannot however provide support for hardware or software failure of such devices.

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 the Designated

Safeguarding Lead (DSL) 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 Lead DSL works with the Network Manager to ensure the monitoring and filtering systems across the site are appropriate and as effective as possible.

Trustees

The Trust Board has overall responsibility within Young Epilepsy for safeguarding the children and young adults that are supported by the organisation. This includes, safeguarding them from online risks.

The Trust Board will be responsible for ratifying the Online Safety Policy and Procedures and monitoring the effectiveness of their implementation.

Governors

Keeping Children Safe in Education (2019) states:

> *As schools and colleges increasingly work online, it is essential that children are safeguarded from potentially harmful and inappropriate online material. As such, governing bodies and proprietors should ensure appropriate filters and appropriate monitoring systems are in place.*

This is also a key theme within the statutory guidance relating to the Prevent Strategy, which aims to stop people being radicalised and drawn into terrorism and extremism.

Keeping Children Safe in Education goes on to say:

> *Whilst filtering and monitoring are an important part of the online safety picture for schools and colleges to consider, it is only one part. Governors and proprietors should consider a whole school approach to online safety.*

Governors and proprietors should ensure that, as part of the requirement for staff to undergo regularly updated safeguarding training and the requirement to ensure children are taught about safeguarding, including online, that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach.

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 safeguarding team.

Visitors

All visitors who wish to access Young Epilepsy's Wi-Fi, will be given a visitor log in to do so. All visitors are provided with an online acceptable use agreement, which they must sign before accessing the Wi-Fi. All online activity across Young Epilepsy's network is then monitored in the same way as outlined earlier in this procedure.

6. DATA PROTECTION

With effect from May 2018, the data protection arrangements for the UK changed following the European Union General Data Protection Regulation (GDPR).

At Young Epilepsy, 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 Young Epilepsy intranet.

7. REPORTING AND MONITORING

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

This procedure will be reviewed annually along with the Online Safety Policy by the Governing Body with advice from the IT and Safeguarding Teams. Staff will be asked to evaluate the effectiveness of the procedures whenever they have had occasion to put them into practice as part of their Refresher Safeguarding Training.

8. PROCEDURE FOR MANAGING UNSUITABLE/INAPPROPRIATE ONLINE ACTIVITY

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from Young Epilepsy and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities that may, generally, be legal but would be inappropriate at Young Epilepsy. 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 & 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 Young Epilepsy 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	
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			

Any online safety concerns from staff, students, volunteers or parents must be passed to the DSL immediately as per the Young Epilepsy Child and Adult Protection and Safeguarding Procedures. 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 DSL or senior managers.

In cases of staff discovering that indecent images of children 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 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 of online safety involving students, will be recorded on the incident reporting system.

If there are concerns about staff's inappropriate use of technology or the internet, Young Epilepsy's other policies and procedures will be followed e.g. Disciplinary Procedure or Managing Allegations Against Staff Procedure.

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:

1. ThinkUKnow - Resources for Teachers, Parents and Young People
2. NCA- CEOP - Child Exploitation and Online Protection Centre
3. Internet Watch Foundation
4. UK Council for Child Internet Safety (UKCCIS)
5. Childnet International
6. UK Safer Internet Centre
7. Parent Info
8. Parentzone
9. SWGfL (South West Grid for Learning)
10. Kidsmart
11. Mencap- Parent's guide to internet safety
12. Surrey Police- internet and phone bullying fact sheet
13. Parents Protect- a guide for parents

14. Young Minds
15. Childline - 0800 1111
16. Action Fraud
17. The professionals Online Safety Helpline (POSH)
18. East Midlands E-Safety Project

Other information

1. E-safety Toolkit (2014), Surrey County Council
2. E-safety Safe Practice with Technology (2009), Surrey County Council
3. Inspecting e-safety in schools (2014), Ofsted
4. Working Together to Safeguard Children (2015), DfE
5. Keeping Children Safe in Education, (2016), DfE
6. Sexting in Schools and Colleges; Responding to incidents and safeguarding young people, (2016), UKCIS
7. Inspecting Safeguarding in Early Years, Education and Skills Settings, (2016), Ofsted
8. Children's online activities, risks and safety: A literature review (2017), UKCIS
9. Education for a Connected World (2018), DfE
10. Digital Resilience Framework (2019), UKCIS

This policy is agreed by the Executive team and will be implemented by all departments.

Date: .....

Signed: .....
Director of Integrated Care

Reviewed January 2020
Next review January 2021
Author: Alex Dave

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 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, photo 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 in order 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 victims 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 cyber crime

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.

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

There were 3.8 million frauds and 2 million cyber crimes 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 cyber crime due to being unaware of such risks and being naïve 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 Young Epilepsy 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 of 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 photo 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 in order to attract the child's attention and interaction, and after doing so will use this trust in order 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.

APPENDIX 2

FAQs

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 Young Epilepsy, 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. Once stored in the appropriate place within Young Epilepsy, the images must then be destroyed/deleted.

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's Child and Adult Protection and Safeguarding Procedures and Whistleblowing Procedures.

Q4. Can I connect my own personal device to Young Epilepsy's Wi-Fi network?

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 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. Young Epilepsy's 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 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:

Other family members accessing the technology inappropriately

Access of adult material- this is never acceptable

Access by others resulting in confidential information about Young Epilepsy, 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 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 How can I use ICT appropriately to communicate with Students?

A9. Staff should not use their personal emails or phone numbers to communicate with children. Staff should use Young Epilepsy technology for this purpose and ensure the tone is professional and cannot be misinterpreted. Staff must only communicate with students via Young Epilepsy email accounts.

APPENDIX 3- Online Safety Risk Assessment Template

This is a template and must be adapted to each individual student

	Risk Assessment Student Access to the Internet on notebook, phone and PC.	**Risk Indicator** *(Before Safety Actions)*			**Safety Actions**	**Risk Indicator** *(After Safety Actions)*		
Hazards	**Risk**	**O**	**S**	**Risk**		**O**	**S**	**Risk**
Disclosure of personal data e.g. real name, dob, addresses, tel nos, financial details, email address to strangers.	Exposure to danger from harmful contact with inappropriate others Grooming Stalking Cyberbullying (either victim or instigator) Cyber crime Fraud				Individual internet access assessment for student Acceptable use protocol/agreement to be read and signed by the student. Instruction on safer behaviour in chat rooms to be provided in key work sessions and student meetings. Instruction on safety measures available in chat rooms. Limited access time (e.g. 6.00pm to 8.00pm). Staff to support when internet is being used.			
Limited understanding of the dangers involved in accessing the internet	Exposure to harmful and/or illegal material or activities from others as above.				Organisational filtering systems in place to prevent access to illegal or harmful sites.			

	Cyber Crime Exploitation Trolling				Staff to support when using mobile device and divert student if inappropriate content is accessed. Staff to report to IT if this happens.			
Inadvertently watching inappropriate content whilst accessing You Tube	Emotional harm				Staff to always supervise when student is using You Tube. Staff to turn off any video that starts on You Tube that is inappropriate- sexual content, profanity or violence.			
Vulnerability to scams and/or phishing	Cyber Crime Fraud Exploitation				Guidance provided by staff to make students aware of scams and phishing. Risks explained in student meeting. Vulnerability to scams/phishing to be considered as part of the individual access assessment and further filtering to be put in place by putting in a request to IT.			

Agreement to meet an individual who student has met online	Exposure to the risk of personal harm				Support and education around safety measures. Student's capacity must be assessed if it is believed they do not have capacity to make this decision to meet someone. Vulnerability to make such an arrangement to be considered as part of the individual access assessment.			
Individual student memory problems	Failure to recall the risks and dangers of online safety Exposure to harm and risks of harm as above as above.				Regular review of access assessment in keywork sessions. Supervision when online in chat rooms. Posters in IT room to remind student of online safety rules.			
Unsolicited contact from strangers	Cyberbullying Grooming Exploitation Cyber crime				Staff to ask student about how they use the internet, what social networking sites are accessed, what games they play and what apps they have. This will help to create an open culture where staff can enquire about the student's use and offer support around this.			

					Support from staff to set up security settings on Facebook account and on WhatsApp. Staff to discuss with student, what to do if someone they have never met face to face, contacts them, or what to do if they see something that worries them.			