**ICT Learner Policy**

**Introduction**

The welfare and security of our young people is the responsibility of all St Eds employees and volunteers. Therefore, everyone should be familiar with and take responsibility for the implementation of these internet guidelines in their own areas of work.

* Learners must be familiar with and conform to these guidelines
* Tutors must be familiar with these guidelines and monitor young people’s internet use to ensure that these guidelines are not breached.
* Tutors must ensure young people are supervised and monitored when accessing the internet
* Tutors should ensure that each young person understands and signs the ‘Rules for responsible internet use’ agreement prior to accessing the internet.
* The Centre Manager should ensure that all staff are familiar with St Eds Internet guidance and ICT Policies

**Online learning**

We follow the guidance on the government website around remote learning and using tools from the SWGfL website (<https://swgfl.org.uk/resources/safe-remote-learning/>). This is to ensure the safety of our learners and the use of the platforms we are using.

When setting up learners from home we have closely followed the guidance on the government website (<https://www.gov.uk/guidance/safeguarding-and-remote-education-during-coronavirus-covid-19>). This is to ensure that we are up to date with any changes or policies surrounding home learning. Since March 2021, we have returned to face-to-face learning, but use remote when necessary.

**Essential Tips to maintain safety and safeguard our learners and colleagues.**

* Colleagues should ensure that they are familiar with the company safeguarding policy and particularly the E-Safety section.
* This can be located via the HR SharePoint site, on the safeguarding tab: <https://skillstrainingukltd.sharepoint.com/sites/HR/Safeguarding/Forms/AllItems.aspx>
* Colleagues should have a clear understanding of the potential risks that may come from learners potentially having more access to sites or sources that increase the possibility of a learner being cyber-bullied, groomed or becoming involved with online radicalisation. As a result, colleagues should regularly discuss and check this with their learners.
* Colleagues should also read and understand the company IT Acceptable Use policy
* All online sessions should be recorded where technology allows, and this should be uploaded with contact evidence.
* Consideration should always be given as to how we will store new personal data from learners and for how long. The Administration department can provide advice regarding this.
* There should be a record or notes detailing how safeguarding has been managed with each learner, especially those that are more vulnerable or have indicated there are issues in their home life.
* Advice should be given to all learners that sessions should take place in the most neutral place in their home. It is recommended that activities should take place not too far away from parents or guardians, if feasible. Always consider the location of learning. Colleagues must consider what can be seen or heard on screen at all times.
* Learners who have indicated they have any history of stress or anxiety may require a different delivery approach. Learner’s levels of stress or anxiety may already be exacerbated by concerns about illness, their financial status or more their future in more general terms for example. It may be useful to deliver in a bite size way, with more frequent contact to provide reassurance whilst not overstretching the learner(s).
* Use this as an opportunity to deliver teaching of good online / e-safety practices.
* Please note that it may be necessary to obtain parent or carer consent for learners to use equipment at home.
* Only use skillstraininguk.com email addresses for learners and not their personal address unless prior authority has been given. Alternatively, learners could use a parent or carer’s email address or account.
* Under no circumstances should a colleague issue their personal email address or phone number to a learner, regardless of the situation.
* All learners should be reminded of Skills Training’s Safeguarding process and be provided with the email address and contact details for those nominated to ensure learners are safeguarded.
* Learners can access details via the Skills Training UK website

**Guidelines**

**Control and Monitoring**

Computers/networks used for Internet access should be fitted with:

* Content filtering facilities to block unsuitable sites
* ESET Anti-Virus or other such software virus protection to block viruses and other malicious software

**Monitoring Process**

* Learners should only be allowed to access St Eds computers and the internet if they have understood and signed the ‘Rules for Responsible Computer and Internet Use’ agreement
* Learners should only be allowed access to the Internet within a supervised and observed environment
* Tutors should ensure they discuss personal safety issues with young people on a regular basis
* During each access session the Tutor should be responsible for supervising access at any given time during that session
* All learner activities are monitored
* Students are given key working sessions around online safety and will highlight if there is a gap in their knowledge/additional concerns that need addressing with further training

**Acceptable Use and Legal Issues**

Internet facilities enable young people to handle a very wide range of information, including personal data, linking to large numbers of computers and other individuals across the world.

In this relatively uncontrolled environment, it is particularly important that young people are aware of and conform to the requirements set out in this document to ensure their security and wellbeing.

Law applying to computer and internet use include:

* The Computer Misuse Act
* The Copyright Act
* Health and Safety at Work Act – Safe Computer Use
* Data Protection Act

Furthermore, the following should also be diligently adhered to:

* Equality Act 2010
* Safeguarding Prevent Duty

Details of these Acts can be found on the internet or you can discuss these with your tutor.

**Specific information for Young People about appropriate Internet access and computer use**

These are the St Eds guidelines and must be followed when using St Eds computers at all times:

* Do not use a computer to harm other people or their work
* Do not damage the computer or the network in any way
* Do not download materials without permission or install any illegal software, shareware or freeware
* Do not view, send, or display offensive messages or pictures
* Do not wasted printer ink and paper
* Do not attempt to access another person’s folders, work or files
* Do tell your Tutor if you are concerned about any materials on the computer
* For your own safety, do not give out any personal information over the Internet or via email unless young have permission to do so from a member of staff
* For your own safety, do not arrange to meet anyone who contacts you over the internet or via email. You should report any contact of this type to a member of staff.
* Discuss with your Tutor which (if any) chatrooms or social networking sites are okay to use. Social networking should not be accessed during learning at St Eds.

**British values and Prevent Agenda**

British values are defined as ‘democracy, the rule of law, individual liberty, and mutual respect and tolerance for those with different faiths and beliefs’

St Eds expects its staff and learners alike to respect these values in the online world and report, in confidence, any perceived deviance from these values.

**Appendix A: Student Code of Conduct for Online Learning**

* Attend all your lessons that you are invited to from your ‘calendar’, join in and complete tasks set
* Arrive on time (Lessons will be open 10 minutes early for you to log in and get set up)
* Be dressed and ready for learning in an appropriate neutral space in your house (not in your bed)
* No music, TV, Gaming whilst in your lessons – please give the tutor your full attention
* No eating or smoking whilst in your lessons
* Please have your video on and ‘pin’ your teacher
* Don’t mute yourself unless asked to do so – have audio on as you enter the classroom
* Only the teacher can end or record a meeting. You will be notified that your lesson is being recorded at the start.
* Be responsible for your behaviour, language use and actions when you are using technology
* Wait your turn – raise your hand to ask a question or type this in the ‘chat’ – the tutor will respond to you as soon as they are able to
* The chat function is for questions only – no private conversations should take place
* Do not be afraid to ask questions if you are unsure of how to use Teams – we will have additional staff on standby for support if you are struggling to work the system
* Please respect your peers and tutors – we are all learning during this pandemic
* Please understand that when using Microsoft Teams and other applications provided by St Edmunds Society that your use can be monitored, logged, and made available to your tutors.

**Appendix B: E-Safety Guidelines**

Always think of your personal safety when first contacting someone you don’t know using ICT or your mobile phone. Remember it’s easy for anyone to lie about who they are online, so you can never really be sure who you are talking to.

Do not give out any personal information about yourself online to someone you don’t know - not your full name, address, street name, postcode, the school/college/Centre you attend or anywhere else you go to near where you live.

Never give your contact number to anyone you don’t know.

It’s a good idea to use a nickname when you are online - never use your real name.

Don’t meet people you have only spoken to online. If you do decide to meet in real life with someone you have met online, make sure you tell your parents, take someone sensible and trustworthy with you and always meet in a public place, at a busy time.

Never give out photographs online or over your mobile unless you know the person in real life. It is easy for someone to alter your photos and send them onto others or, even, to use them to pretend they are you!

Always use private settings whenever setting up a social network page or an Instant Messenger account, so your personal details can’t be seen by people you don’t know.

Anything you upload to the Internet will be there forever, so be careful what you put online.

Never go onto a webcam session with people you don’t know in real life. Webcam images can be recorded, copied and shared with other people.

If you receive any messages or photos that worry or upset you, talk to your parents or a trusted friend.

You can also report it online via the website:

[www.thinkyouknow.co.uk](http://www.thinkyouknow.co.uk)

Mobile Phone Safety

Remember if you are being bullied it isn’t your fault. Talk to a trusted adult at home or at St-Eds.

Don’t reply to any nasty messages you receive as this could lead to further messages

Don’t reply to a text from someone you don’t know.

Keep the messages you have been sent so you can show them to a trusted adult and make a note of the time and date of the messages or calls you receive

Don’t answer calls form withheld numbers or numbers you don’t recognise, let it go to voicemail.

Block numbers from people who are sending you nasty messages/calls

If you are bullied repeatedly, speak to someone who can change your number

Don’t give out your mobile number to someone you don’t know

Don’t send pictures to someone you don’t know, especially of yourself or of others

What should you do if you are being bullied online?

Tell an adult you trust if you are being cyberbullied

Don’t respond or retaliate to bullying messages – it could make things worse. Block users who send you nasty messages

Save abusive emails or messages (or texts) you receive

Make a note of dates and times you receive bullying messages, as well as details you have of the user’s ID and the URL

Don’t pass on any cyberbullying videos or messages – this is cyberbullying. If you are bullied repeatedly change your use ID, or profile, and use a name that doesn’t give any information away about you

If any of the above is affecting you and the problem is serious, you can report it to the police, cyber mentors, or ChildLine

[www.thinkUknow.co.uk](http://www.thinkUknow.co.uk)

[www.cybermentors.org.uk](http://www.cybermentors.org.uk)

[www.childline.org.uk/talk/pages/talk.aspx](http://www.childline.org.uk/talk/pages/talk.aspx)