ICT and Online Safety 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.

The purpose of this policy statement is to:

- Ensure the safety and wellbeing of our students whilst they are using the internet, social media or mobile devices
- Provide staff and volunteers with the overarching principles that guide our approach to online safety
- Ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

The policy statement applies to all staff, volunteers, students and anyone involved in St Edmunds Society activities.

- 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 General Manager should ensure that all staff are familiar with St Eds Internet guidance and ICT Policies

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.

We recognise that:

- The online world provide everyone with many opportunities; however it can also present risks and challenges
- We have a duty to ensure that all young people involved in our organsiation are protected from potential harm online.
- All young people, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse
- Working in partnership with young people, their parents, carers and other agencies is essential in promotion young people's welfare and in helping young people to be responsible in their approach to online safety.

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 waste 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.
- Do not access social networking during learning at St Eds.
- Do not access social media whilst at St Eds.
- Do not take photos or videos whilst at St Eds. This includes photos or videos which have staff or other students in them.

<u>At St Eds, we do not tolerate the following:</u>

- **Students sending threatening messages online** (via any platform) to any other student. Threatening messages can look like
  - Telling others that you will arrange for them to be beaten up
  - Telling others that you know where they live and that you will go and hurt them
  - Telling others that you will hurt them at St Eds, or outside St Eds
  - Telling others that they will "get jumped".

- Student's harassing other students online. Harassment can include things like **verbal abuse, bullying, jokes, making faces and posting comments about you on social media**. It also includes sexual harassment.

- Students sending antagonising messages to others.

If students receive any messages of the above criteria, it must be reported. Rather than responding to these messages (with threats or antagonising) please screenshot the message and then block said person. Please then inform Welfare who will support.

If you do send threatening messages, it will be reported to the police. You need to be aware that any evidence of this could put your course placement at risk. We will also need to inform your guardian.

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.

<u>E-Safety Guidelines</u>

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

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

www.cybermentors.org.uk

www.childline.org.uk/talk/pages/talk.aspx