



UTC South Durham

E-safety Policy



Date of adoption	June 2022
Approved by	Governing Body

Signed: (Principal) 	Date: 10 June 2022
Signed: (Chair of Governors) 	Date: 10 June 2022

Date to be reviewed by	June 2024
Review History	Reviewed – Tom Dower Oct 19 Reviewed – Tom Dower Nov 20 Reviewed – Catherine Purvis-Mawson, April 2022
Responsibility	Principal

1. Introduction

E-safety encompasses the use of new technologies, internet and electronic communications such as mobile phones and tablets, collaboration tools, social networking and personal publishing. It highlights the need to educate students, parents and staff about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

While students' confidence in the use of technology increases it becomes more important that we control its use within UTC and educate students and staff about using it safely outside of the UTC.

The UTC's E-safety Policy will operate in conjunction with other policies including those for Behaviour, Safeguarding, Preventing Bullying, Data Protection and the staff and student Acceptable Use Policy (AUP).

E-safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies
- Sound implementation of the E-safety Policy in both administration and curriculum, including secure UTC network design and use
- Safe and secure broadband filtering

The UTC's E-safety Co-ordinator is Tom Dower.

2. Teaching and learning

2.1 Why internet use and technology is important

- The internet and use of new technology are essential elements in 21st century life for education, business and social interaction. The UTC has a duty to provide students with quality internet access as part of their learning experience
- Internet use is a part of the curriculum and a necessary tool for staff and students. The use of computers, tablets and mobile phones can also enhance the education of our students and should be encouraged as long as suitable controls are in place
- Students and staff use the internet widely outside the UTC and need to learn how to evaluate internet information and to take care of their own safety and security

2.2 Internet use will enhance learning

- The UTC internet access is designed expressly for student use and includes filtering appropriate to the age of students
- Students will be taught what internet use is acceptable and what is not and given clear objectives for internet use
- Students will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation

2.3 Students will be taught how to evaluate internet content

- The UTC will ensure that the use of internet derived materials by staff and students complies with copyright law

- Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy
- Students will be taught about plagiarism and why this is not acceptable

3. Managing internet access and technology

3.1 Information system security

- UTC ICT systems capacity and security will be reviewed regularly
- Virus protection will be updated regularly
- Cyber security considerations have also been assessed and relevant checks made to ensure if a cyber-attack does occur that safeguards and appropriate measures can be implemented

3.2 Email and mobile communication

- Students may only use approved email accounts on the UTC system, such as the email embedded in Office 365. This will be administered and monitored by UTC staff or contractors. Post-16 students may use personal emails when needed for work purposes, such as for UCAS applications
- Students must immediately tell a member of staff if they receive offensive email communications
- Students must use email responsibly – the normal UTC behaviour rules apply. They should use it only for UTC communication
- Staff should only use their UTC email accounts for business purposes. Email sent to parents or an external organisation should be written carefully, in the same way as a letter written on UTC headed paper
- Staff should never use personal email accounts in communication with students or parents
- The forwarding of chain letters is not permitted.
- Personal mobile phone numbers should not be used by staff to contact parents or students. If this is unavoidable then the E-safety Co-ordinator or a DSL should be informed promptly. Staff may have work email, calendars and documents on mobile devices or tablets subject to having passcode protection in place. Under these circumstances, staff should not share their passcode with anyone else, nor let them use the device. They should be aware that if they lose the device while it is unlocked then their information is unprotected; suitable care should be taken and the E-safety Co-ordinator informed in such an event.

3.3 Published content and the UTC website

- The contact details on the website should be the UTC address, email and telephone number. Staff or students' personal information will not be published
- The E-safety Co-ordinator will take overall editorial responsibility and ensure that content is accurate and appropriate

3.4 Publishing students' images and work

- Photographs that include students will be selected carefully and will not enable individual students to be clearly identified
- Students' full names will not be used anywhere on the UTC website in association with photographs
- Written permission from parents or carers will be obtained before photographs of students are published on the UTC website

3.5 Social networking and personal publishing

- The UTC will block/filter access to social networking sites unless approved by the E-safety Co-ordinator. Access to social networking will be controlled by the IT support team and will be used for educational purposes
- Students will be advised never to give out personal details of any kind which may identify them or their location
- Students and parents/carers will be given guidance on the use of social network sites outside the UTC and this should be age-appropriate
- Staff should never communicate with students through social networking sites outside the UTC; we have good quality internal communication systems for that. If this is necessary (eg due to involvement in external clubs) then the Designated Person for Child Protection should be informed
- Staff should be thoughtful and responsible in their personal use of social networking (see Code of Conduct) and ensure that they do not compromise themselves or the UTC. In particular, care should be taken in interaction with parents, ex-students and other members of the local community. Staff must not mention students or disclose any confidential information about the UTC. Any 'friend requests' from students should be declined and blocked. Any concerns should be raised with the E-safety Co-ordinator
- Social networking may be used by staff for student communication but only if it is set up formally using UTC accounts, it is carefully monitored and the E-safety Co-ordinator is fully aware
- Staff should ensure that they take appropriate security measures when using external social networking sites so that they protect themselves (e.g. privacy settings)

3.6 Managing filtering

- The UTC will work with the IT Managed Service company and the Internet Service Provider to ensure systems to protect students are reviewed and improved
- If staff or students discover an unsuitable site, it must be reported to the E-safety Co-ordinator or IT Managed Service company
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable, to ensure high quality education while keeping students safe
- All computer use within UTC and on UTC-owned devices will be monitored using Smoothwall software or an equivalent
- Use of internet and the network will be monitored and controlled in lessons by staff using AB Tutor or equivalent

3.7 Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in UTC is allowed
- Mobile phones will not be used during lessons or formal UTC time unless permission is expressly given by a teacher. Normal UTC sanctions apply to the use of technology (e.g. the sending of abusive or inappropriate text messages)
- The use of the UTC wireless networks by staff, students and visitors are only permitted by following the UTC's procedures and a suitable AUP signed by the user

3.8 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and GDPR regulations 2018
- Student and staff personal data will not be displayed, physically or electronically, in public areas or areas where visitors or students have access
- Access to the UTC's MIS systems will be password protected. Staff should always lock computers when they leave them unattended

4. Policy decisions

4.1 Authorising internet access

- All staff must read and sign the AUP before using any UTC ICT resource
- The UTC will keep a record of all staff who are granted internet access. The record will be kept up-to-date
- At the UTC, all students must read and sign the AUP before using any UTC ICT resource
- Visitors to the UTC will sign an AUP if they are going to use the UTC's ICT resources or internet unsupervised

4.2 Assessing risks

- The UTC will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a UTC computer
- The UTC will audit ICT provision to establish if the E-safety Policy is adequate and that its implementation is effective

4.3 Handling e-safety incidents and complaints

- Incidents and complaints of internet misuse will be dealt with by the E-safety Co-ordinator or another senior member of staff
- Any incident or complaint about staff misuse must be referred to the Principal and may be referred to the LADO
- Incidents and complaints of a child protection nature must be dealt with in accordance with UTC Safeguarding procedures

4.4 Dealing with cyber bullying

- Cyber bullying (along with all forms of bullying) will not be tolerated in UTC. Full details are set out in the UTC's Preventing Bullying Policy
- Support will be available for anyone affected by cyber bullying
- Incidents or allegations of cyber bullying will be thoroughly investigated. The police will be contacted if a criminal offence is suspected
- All incidents of cyber bullying reported to the UTC will be recorded

4.5 Bring your own device (BYOD)

- We wish to encourage the use of students' own devices. This gives students agency in their use of technology which is important as we treat them as young adults and prepare them for work. For many students, using their own device will be more efficient and develop their organisational skills and sense of responsibility
- Students bringing their own device must register them with the IT Technician. Laptops which are to be allowed onto the school system will have monitoring software installed. More likely students will have access to the internet only where they can use Office 365 and the cloud based file storage and communication systems
- All students will have lockers and there will be charging points available throughout the building. Students bring their devices at their own risk. The UTC cannot take responsibility for any damage to personal equipment

5. Communications Policy

5.1 Introducing the E-safety Policy to students

- E-safety rules will be posted in all networked rooms and discussed with the students at the start of each year
- Students will be informed that network and internet use will be monitored
- An E-safety training programme will be in place for all students (initially as part of their induction)

5.2 Staff and the E-Safety Policy

- The E-Safety Co-ordinator will undergo suitable training (eg CEOP, LA courses) and ensure that appropriate members of staff have CPD to be able to carry out their jobs effectively. All staff will be given the UTC E-safety Policy and its importance explained
- E-safety will be covered as part of staff Child Protection/Safeguarding training every year for all staff
- To protect all staff and students, the UTC will implement AUPs
- Staff will be made aware that computer usage and internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential

5.3 Enlisting parents' support

- Parents' attention will be drawn to the UTC E-safety Policy in newsletters and on the UTC website
- Appropriate training will be offered to parents and information updates sent home on a regular basis
- Parents will receive advice about supporting their children in the safe use of ICT

5.4 Prevent

- Staff should be aware of the dangers of radicalisation in students and in particular that the process of grooming a young person can be accelerated through contact on line and access to extremist materials can be easier through the internet
- If staff are concerned about a student they must report it to the DSL