

UTC Swindon
e-SAFETY POLICY

Author: Deputy Principal	Version: 1
Date approved:	Date reviewed:
Comments:	
Monitoring, evaluation and review: The Principal and Board of Directors will review this policy at least every two years and assess its implementation and effectiveness. The policy will be promoted and implemented throughout by UTC Swindon.	

Policy implementation and oversight

UTC Swindon has an e–Safety Coordinator. This person liaises with the Designated Child Protection Officer as and when the roles overlap.

1. Teaching and learning

1.1 Why is Internet use important?

- Internet use is part of the statutory curriculum and a necessary tool for learning
- The Internet is a part of everyday life for education, business and social interaction. The College has a duty to provide students with quality Internet access as part of their learning experience
- Students use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security
- The purpose of Internet use at UTC Swindon is to raise educational standards, to promote student achievement, to support the professional work of staff, to support its digital specialism and to enhance the College's management functions
- Internet access is an entitlement for students who show a responsible and mature approach to its uses.

1.2 How does Internet use benefit education?

Benefits of using the Internet in education include:

- Access to worldwide educational resources;
- Educational and cultural exchanges between students worldwide;
- Vocational, social and leisure use in libraries, clubs and at home;
- Access to experts in many fields for students and staff;

- Professional development for staff through access to national developments, educational materials and effective curriculum practice;
- Collaboration across networks of schools, support services and professional associations;
- Improved access to technical support including remote management of networks and automatic system updates;
- Exchange of curriculum and administration data with DfE;
- Access to learning wherever and whenever convenient.

1.3 How can Internet use enhance learning?

- UTC's Internet access will be designed to enhance and extend learning;
- Students will be taught what is and is not acceptable in terms of Internet use and given clear objectives for Internet use and sign an Acceptable Use of ICT User Agreement;
- UTC will ensure that the copying and subsequent use of Internet derived materials by staff and students complies with copyright law;
- Access levels will be reviewed to reflect the curriculum requirements and age of students;
- Staff should guide students to online activities that will support the learning outcomes planned for the students' age and maturity;
- Students will be supported in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation;
- Students will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

1.4 How will students learn how to evaluate Internet content?

Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. This will take place during ICT lessons, however, the evaluation of online materials is a part of teaching/learning in every subject.

2. Managing information systems

2.1 How will information systems security be maintained?

- The security of UTC MIS and users will be reviewed regularly
- Virus protection will be updated regularly
- Personal data sent over the Internet or taken off site will be encrypted
- Portable media may not be used without specific permission followed by a virus check
- Unapproved software will not be allowed in students' work areas or attached to email
- Files held on the school's network will be regularly checked
- The ICT coordinator/network manager will review system capacity regularly

2.2 How will email be managed?

- Students may only use approved email accounts
- Students must immediately tell a teacher if they receive offensive email
- Students must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from a member of staff
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper
- The forwarding of chain messages is not permitted
- Staff should only use school email accounts to communicate with students

2.3 How will published content be managed?

- The contact details on the website are the UTC address, email and telephone number. Staff or students' personal information must not be published
- The Principal will take overall editorial responsibility and ensure that content is accurate and appropriate. This task will be delegated as appropriate.
- Images that include students will be selected carefully and will not provide material that could be reused
- Students' full names will not be used anywhere on the website, particularly in association with photographs
- Written permission from parents or carers will be obtained before images of students are electronically published
- Students' work can only be published with their permission of parents/carers

2.4 How will social networking, social media and personal publishing be managed?

- The UTC will control access to social media and social networking sites.
- Students will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Students should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location.
- Staff official blogs or other posts should be password protected and run from the UTC website with approval from the SLT. Staff should be advised not to run social network spaces for student use on a personal basis.
- If personal publishing is to be used with students then it must use age appropriate sites suitable for educational purposes. Personal information must not be published and the site should be monitored by UTC staff.
- Students should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications.
- Students should be encouraged to invite known friends only and deny access to others by making profiles private.
- Students are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

2.5 How will filtering be managed?

- UTC will work with our designated ICT support providers to ensure that systems to protect students are reviewed and improved
- If staff or students discover unsuitable sites, the url must be reported to the e-safety coordinator
- The UTC broadband access includes filtering appropriate to the age and maturity of students
- Appropriate staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable
- Any material that the UTC believes is illegal must be reported to appropriate agencies

- The UTC's access strategy will be designed by staff to suit the age and curriculum requirements of the students, with advice from network managers

2.6 How will emerging technologies be managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in UTC is allowed
- Mobile phones may be used to support learning in lessons with staff permission. The sending of abusive or inappropriate text, picture or video messages is forbidden. Acceptable use of mobile phones forms part of the Code of Conduct and Home College Agreement

2.7 How should personal data be protected?

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

2.8 How will video conferencing be managed?

- All video conferencing equipment in the classroom must be switched off when not in use and not set to auto answer
- Equipment connected to the educational broadband network should use the national E.164 numbering system and display their H.323 ID name
- External IP addresses should not be made available to other sites
- Video conferencing contact information should not be put on the UTC website
- The equipment must be secure and if necessary locked away when not in use
- UTC video conferencing equipment should not be taken off school premises without permission

2.9 Users

- Students should ask permission from the supervising teacher before making or answering a video conference call.
- Video conferencing should be supervised appropriately for the students' age.
- Parents and carers should agree for their children to take part in video conferences.
- Only key administrators should be given access to video conferencing administration areas or remote control pages.
- Unique log on and password details for the educational video conferencing services should only be issued to members of staff and kept secure.

2.10 Content

- When recording a video conference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of video conference should be clear to all parties at the start of the conference. Recorded material shall be stored securely
- Video conferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity
- If third party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights
- Establish dialogue with other conference participants before taking part in a video conference. If it is a non school site it is important to check that they are delivering material that is appropriate for your class

3. Policy decisions

3.1 How will Internet access be authorised?

- UTC will maintain a current record of all staff and students who are granted access to the College's electronic communications

- All staff must read and sign the 'UTC Staff ICT User Agreement' before using any school ICT resources
- Parents/carers will be informed that students are provided with supervised Internet access

3.2 How will risks be assessed?

- UTC will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a College computer. UTC cannot accept liability for the material accessed, or any consequences resulting from Internet use
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990
- Methods to identify, assess and minimise risks will be reviewed regularly

3.3 How will e–Safety complaints be handled?

- Complaints of Internet misuse will be dealt with under the College's Complaints Procedure
- Any complaint about staff misuse must be referred to the Principal
- All e–Safety complaints and incidents will be recorded by UTC — including any actions taken
- Students and parents/ carers will be informed of the Complaints Procedure
- Parents/carers and students will work in partnership with staff to resolve issues
- Support will be sought with the local Police to establish procedures for handling potentially illegal issues.
- Any issues (including sanctions) will be dealt with according to the College's disciplinary and child protection procedures

3.4 How is the Internet used across the community?

- The UTC will liaise with its partners to establish a common approach to e–Safety.
- UTC will be sensitive to Internet related issues experienced by students outside College e.g. social networking sites, and offer appropriate advice.

3.5 How will Cyberbullying be managed?

- Cyberbullying (as with all forms of bullying) will not be tolerated in UTC. Full details are set out in the UTC policy on anti-bullying
- There will be clear procedures in place to support anyone affected by cyberbullying
- All incidents of cyberbullying reported to UTC will be recorded
- There will be clear procedures in place to investigate incidents or allegations of cyberbullying
- Students, staff and parents/carers will be advised to keep a record of the bullying as evidence
- UTC will take steps to identify the bully, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary
- Sanctions for those involved in cyberbullying as set out in the UTC Behaviour Policy
- The Police will be contacted if a criminal offence is suspected.

3.6 How will Learning Platforms and learning environments be managed?

- Usage of the LP by students and staff will be monitored regularly in all areas, in particular message and communication tools and publishing facilities
- Students/staff will be advised on acceptable conduct and use when using the LP

- Only members of the current student, parent/carers and staff community will have access to the LP
- All users will be mindful of copyright issues and will only upload appropriate content onto the LP
- When staff, students etc leave UTC their account or rights to specific College areas will be disabled or transferred to their new establishment
- Any concerns with content may be recorded and dealt with in the following ways:
 - The user will be asked to remove any material deemed to be inappropriate or offensive
 - The material will be removed by the site administrator if the user does not comply
 - Access to the LP for the user may be suspended
 - Parents/Carers may be informed
- A visitor may be invited to use the College LP by a member of SLT. In this instance there may be an agreed focus or a limited time slot
- Students may require editorial approval from a member of staff. This may be given to the student to fulfil a specific aim and may have a limited time frame

4. Communication policy

4.1 How will the policy be introduced to students?

- All users will be informed that network and Internet use will be monitored.
- An e-Safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use
- Student instruction in responsible and safe use should precede Internet access.
- An e-Safety module will be included in the ICT schemes of learning, covering both safe College and home use
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum. Particular attention will be given where students are considered to be vulnerable

4.2 How will the policy be discussed with staff?

- The e-Safety Policy will be formally provided to all members of staff
- To protect all staff and students, UTC will implement Acceptable Use Policies
- Staff should be aware that Internet traffic can be monitored and traced to the individual user, Discretion and professional conduct is essential
- Staff that manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues
- Staff training in safe and responsible Internet use both professionally and personally will be provided.

4.3 How will parent/carers' support be enlisted?

- Parents' attention will be drawn to UTC e-Safety Policy in newsletters, the UTC prospectus and on the College website.
- A partnership approach with parents/carers will be encouraged. This will include parent information evenings with demonstrations and suggestions for safe home Internet use