UTC LEEDS
UNIVERSITY TECHNICAL COLLEGE

UTC Leeds
E-Safety Policy

Adopted by the Governing Board on: February 2021

To be reviewed by Governors on: February 2022

SLT: Alex Berry
Governor link: Tim Craven

1. Policy implementation and oversight

UTC Leeds has an e–Safety Coordinator. This person liaises with the Designated Child Protection Coordinator as and when the roles overlap. The purpose of this policy is to protect UTC Leeds against information vulnerabilities and prevent unauthorised data access, loss or disclosure.
This policy applies to anyone who is accessing the UTC Leeds information, systems and buildings.

2. Core Principles

- The IT Manager will have overall accountability for managing the IT estate;
- We will ensure our school has a database of information assets and staff accountable for those assets;
- We will ensure our school has a recognised process for identifying and investigating information incidents and breaches - please see the UTC Leeds Data Protection policy in addition to the information in this policy;
- We will ensure information is safely & securely disposed of after it reaches its retention period
- We will ensure electronic devices and removable media are wiped clean and disposed of securely at the end of their use
- We will have plans in place to ensure the continuity of our school business in the event of an unforeseen incident occurring;
- We will ensure all personal data on portable UTC Leeds devices and media is encrypted
- We will ensure that we make regular back-ups of our data held on electronic devices and systems
- We will ensure we are satisfied and assured about the people who are working for our school before giving them access to our information e.g. references, vetting, clauses in contracts etc.

3. Teaching and learning

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 school 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 Leeds 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 school’s management functions
- Internet access is an entitlement for students who show a responsible and mature approach to its use

How does Internet use benefit education?

Benefits of using the internet in education include:

- Access to worldwide educational resources including museums and art galleries;
- 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 and LCC
- Access to learning wherever and whenever convenient.

How can internet use enhance learning?

UTC Leeds' internet access will be designed to enhance and extend education:

- Students will be taught what is and is not acceptable in terms of internet use and given clear objectives for internet use.
- UTC Leeds will ensure that the copying and subsequent use of internet derived materials by staff and students complies with copyright law.
- Access levels 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 educated 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

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 responsibility of teaching/learning in every subject.

4. Managing information systems

How will information systems security be maintained?

- The security of the school information systems 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
- Files held on the school's network will be regularly checked
- The ICT coordinator/network manager will review system capacity regularly
  Lock down process implemented for ransomware attacks

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
- Staff wil only use school email accounts to communicate with students

How will published content be managed?

- The contact details on the website are UTC Leeds 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

Can students' images or work be published?

- Images that include students will be selected carefully and will not provide materials to third parties for re-use
- 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 or the parents

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

□ **UTC Leeds** 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, instant messaging address and email addresses, full names of friends/family, specific interests and clubs etc.
- Students will 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 wikis will be password protected and run from the school website with approval from the SLT. Staff should be advised not to run social network spaces for student use on a personal basis.
- Students and staff will be advised on security and enforced through agreed rules to set and change passwords. They will be taught to 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.

How will filtering be managed?

- UTC Leeds will work with our designated ICT support providers to ensure their advice regarding our systems is implemented to protect students.
- If staff or students discover unsuitable sites, the url must be reported to the e–safety coordinator or ICT.
- UTC Leeds firewall includes filtering appropriate to the age and maturity of students
- The e-safety co-ordinator will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that UTC Leeds believes is illegal must be reported to appropriate agencies
- UTC Leeds access strategy for educational content will be designed by educators to suit the age and curriculum requirements of the students, with advice from network managers

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 Leeds is allowed
- Mobile phones may be used to support learning in lessons. 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 School Agreement

How should personal data be protected?

Personal data will be recorded, processed, transferred and made available according to UTC Leeds Data Protection policy

How will videoconferencing be managed?

- All videoconferencing 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
- Videoconferencing contact information should not be put on the school website
- The equipment must be secure and, if necessary, locked away when not in use
- UTC Leeds video conferencing equipment should not be taken off school premises without permission

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 videoconferences.
- Only key administrators should be given access to videoconferencing administration areas or remote control pages.
- Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure.

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 videoconference. If it is a non-school site it is important to check that they are delivering material that is appropriate for your class

5. Policy decisions

How will internet access be authorised?

- UTC Leeds will maintain a current record of all staff and students who are granted access to the school's network and internet
- All staff must read and sign the 'UTC Leeds Acceptable Use Policy' before using any
- school ICT resources Parents will be informed that students will be provided with

How will risks be assessed?

- UTC Leeds 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 school computer. UTC Leeds 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

How will e–Safety complaints be handled?

- Any e-safety complaints will be dealt with under the UTC Leeds' Complaints Procedure
- Any complaint about staff misuse of the UTC Leeds IT equipment must be referred to the Principal

Students and parents will be informed of the complaints procedure

How is the internet used across the community?

- The school will be sensitive to internet related issues experienced by students out of school, e.g. social networking sites and offer appropriate advice.

How will cyberbullying be managed?

- Cyberbullying (along with all forms of bullying) will not be tolerated in school. Full details are set out in the UTC's policy on anti-bullying
- There will be clear procedures in place to support anyone affected by cyberbullying
- All incidents of cyberbullying reported to UTC Leeds will be recorded & monitored

How will Learning Platforms and learning environments be managed?

- E-safety co-ordinator will monitor the usage of the Managed Learning Environment (MLE) by students and staff 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 MLE
- Only members of the current student and staff community will have access to the MLE
- All users will be mindful of copyright issues and will only upload appropriate content onto the MLE
- When staff, students etc. leave UTC Leeds, their account or rights to specific school areas will be disabled
- When staff change roles their permissions and access will be reviewed to ensure they remain relevant and appropriate.
- 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 MLE for the user may be suspended
    - Parents/carers may be informed
- A visitor may be invited onto the MLE 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

6. Communication policy

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 student learning, covering both safe school and home use
- e–Safety training will be part of the induction training into the UTC regardless of start date.

- 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

How will the policy be discussed with staff?

- The e–Safety Policy will be made available to all members of staff
- To protect all staff and students, UTC Leeds 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 e-safety co-ordinator and have clear procedures for reporting issues
- Staff training in safe and responsible internet use both professionally and personally will be provided.

How will parents' support be enlisted?

Parents' attention will be drawn to UTC Leeds e–Safety Policy on the school website. A partnership approach with parents will be encouraged

7. Remote working

- If staff working are away from the office, they will only take the minimum physical information required;
- If staff are transporting physical information, they will ensure it is kept out of sight and secure;
- If staff are working from home, they will ensure the school's information is kept private from family members and ensure there is a secure authentication process;
- Staff must not put personal data on their own devices

-

8. Physical Security

We will ensure appropriate physical information that contains personal data is always stored in either locked filing cabinets and/or locked offices;

- We will ensure staff lock the screen of their PC whenever they are away from their desk;
- We will ensure access to non-public accessible areas in buildings is controlled;
    - All visitors sign in when arriving and out when leaving
    - All visitors are escorted through the building by a member of staff
    - Appropriate access locks are fitted to areas of the building containing sensitive information
    - Ensure all staff are wearing identification badges
- When vacating or moving offices, we will undertake a thorough sweep of the building to ensure all information has been removed – check left over furniture, basements, lofts etc.;
- We will ensure paper records are disposed of securely using a cross-cutting shredder or a reputable confidential waste company