



## E-Safety Policy



North East Futures UTC has been established to change the education, skills and employment paradigm in our IT and Healthcare Science sectors in the North East. It provides the opportunity for young people from all the communities in this region to benefit from its specialist provision.

Local Governors and all the North East Futures staff are committed to a policy of equality and aim to ensure that all students, employees, job applicants, other member of the school community and visitors are treated fairly and with respect.

We aim to give equal access to the high quality educational opportunities we provide and to ensure that everyone feels that they are a valued member of the school community. We seek to create a safe and happy environment where all our students can flourish and where social and cultural diversity are celebrated.

|  |  |
|--|--|
| Reviewed by:                             | Principal and Trustees   |
| Frequency of policy review:              | Biennially   |
| Lead Sub Committee for discussion:       | Educational Standards  |
| Last Reviewed:                           | June 2018  |
| By Dan Sydes                             |  |
| Ratified by Local Board of Governors on: | 6 <sup>th</sup> June 2018  |
| By Michael Whitaker                      |  |
| Next Review Date:                        | May 2020   |

### 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.

As 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, Child Protection, Anti Bullying, Data Protection and the staff and student and staff Acceptable Use Agreement (AUA).

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 Coordinator is Dan Sydes.

### 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.

#### 2.2. Internet use will enhance learning

- UTC internet access is designed expressly for student use and will include 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. This will be delivered primarily through the pastoral programme and Personal Development sessions.
- Students will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation. This will be delivered primarily through the independent learning programme

### 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

### 3.2. Email and mobile communication

- Students may only use approved email accounts on the UTC system, all with @NEFuturesutc.co.uk as the suffix. This will be administered and monitored by UTC staff.
- Students must immediately tell a member of staff if they receive offensive email
- Students must use email responsibly – the normal UTC rules apply. They should use it only for UTC communication and should use a UTC signature and disclaimer.
- Staff should only use their UTC email accounts for business purposes.
- Email sent to parents/carers or an external organisation should be written carefully, in the same way as a letter written on UTC headed paper. Training will be provided if needed.
- Staff should not use personal email accounts in communication with students or parents
- Staff should use UTC telephones wherever possible when communicated with external stakeholders.
- Staff may have work email, calendars and documents on mobile devices or tablets subject to agreed level of password protection. Under these circumstances, staff should not share their password 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 Coordinator informed in such an event.

### 3.3. Published content and the UTC website

- The contact details on the website should be the UTC address, emails 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

- Consent must be obtained from parents/carers and students before publishing any photographic or video media containing their image
- Students' full names will not be used anywhere on the UTC website in association with photographs

### 3.5. Social networking and personal publishing

- The UTC will prevent access to social networking sites unless approved by the E-safety Coordinator. 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 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 personal social networking sites.
- Staff should be thoughtful and responsible in their personal use of social networking (see Acceptable Use Agreement) 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 'requests' from students should be declined and blocked. Any concerns should be raised with the E-safety Co-ordinator.
- Social networking communication it is set up formally using official UTC accounts, it is carefully monitored and the E-safety Coordinator will be made fully aware
- Staff should ensure that they take appropriate security measures when using external social networking sites so that they protect themselves (through privacy settings). Staff should seek advice or guidance on this matter whenever needed

### 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 accessible from the UTC network, it must be reported to the E-safety Coordinator
- Senior staff will ensure that regular checks are made to ensure that the filtering and preventive methods selected are appropriate, effective and reasonable, to ensure high quality education while keeping students safe
- All ICT use within UTC and on UTC-owned devices will be monitored using Smoothwall or an equivalent. A weekly summary report will be reviewed by the E-safety Coordinator.

### 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 member of staff. Normal UTC sanctions apply to the misuse of technology. See the Behaviour Policy for more details
- The use of the UTC wireless networks by staff, students and visitors are only permitted by following the UTC's procedures and a suitable Acceptable Use Agreement signed by the user

## North East Futures UTC – E-Safety Policy

### 3.8. Protecting personal data

- Personal data will be recorded, processed, transferred, protected and made available according to the Data Protection Act 1998 and GDPR guidelines
- 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 BROMCOM MIS system will be password protected. Staff should always lock computers when they leave them unattended.

## 4. Policy decisions

### 4.1. Authorising internet access

- All staff and students must read and sign the Acceptable Use Agreement before using any UTC ICT resource
- Visitors to the UTC will sign an Acceptable Use Agreement in order to have guest Access to the WiFi facilities and use will be monitored

### 4.2. Assessing risks

- The UTC will take all reasonable precautions to ensure that users access only appropriate material. However, due to the scale of content, it is not possible to guarantee that unsuitable material will never appear on a UTC computer
- If unsuitable material is accessed by any member of staff, student or visitor it should be reported to the E-Safety Coordinator
- 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 initially by the E-safety Coordinator and follow the UTC Complaints Policy
- Any incident or complaint about staff misuse must additionally 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 Child Protection Policy

### 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 Anti- Bullying Policy.

## North East Futures UTC – E-Safety Policy

### 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 will develop their organisational skills and sense of responsibility.
- Internet access is provided by the UTC network and BYOD devices are subject to the same monitoring and filtering of content and are restricted in access to non-essential Ports
- Students using BYOD are subject to the same Activity Use Agreement and Behaviour Policy as students using UTC devices
- 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 guidelines will be visible through the Digital Signage system
- Students will be informed and reminded that network and internet use will be monitored and of the AUA expectations
- An E-safety training programme will be in place for all students (initially as part of their induction and then ongoing as part of the Pastoral programme)

### 5.2. Staff and the E-Safety Policy

- The E-Safety Coordinator will undergo suitable training; all staff will receive internal training on E-Safety and all staff will be given access to the UTC E-safety Policy.
- E-safety will be also covered as part of staff Child Protection training every year for all staff
- To protect all staff and students, the UTC will implement Activity Use Agreements and signed copies will be kept in student and staff files
- Staff will be made aware that computer usage and internet traffic can be monitored and traced to the individual user and that discretion and professional conduct is essential and expected.

### 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