Liverpool Life Sciences UTC

Electronic Communication and e-Safety

INTRODUCTION

Liverpool Life Sciences UTC recognises that the use of information and communication technologies in schools brings great benefits. Recognising the e-Safety issues and planning accordingly will help to ensure appropriate, effective and safer use of electronic communications.

Why does a School or Setting need an e-Safety Policy?

In today’s society, children, young people and adults interact with technologies such as social networking, mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

E-Safety covers issues relating to children and young people as well as adults and their safe use of the internet, mobile phones and other electronic communications technologies, both in and out of school. It includes education for all members of the school community on risks and responsibilities and is part of the ‘duty of care’ which applies to everyone working with children.

Schools and other settings must decide on the right balance between controlling access to the internet and technology, setting rules and boundaries and educating students and staff about responsible use. Schools must be aware that children and staff cannot be completely prevented from being exposed to risks both on and offline. Students should be empowered and educated so that they are equipped with the skills to make safe and responsible decisions as well as to feel able to report any concerns. All members of staff need to be aware of the importance of good e-Safety practice in the classroom in order to educate and protect the children in their care. Members of staff also need to be informed about how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role.

Breaches of an e-Safety policy can and have led to civil, disciplinary and criminal action being taken against staff, Students and members of the wider school community. It is crucial that all settings are aware of the offline consequences that online actions can have.

Schools must be aware of their legal obligations to safeguard and protect children on and offline and the accountability of these decisions will sit with the Principal and the Governing body.

The e-Safety policy is essential in setting out how the school plans to develop and establish its e-Safety approach and to identify core principles which all members of the school community need to be aware of and understand.

2 TEACHING AND LEARNING

2.1 Why is Internet use important?

Internet use is part of the statutory curriculum and is a necessary tool for learning.

The Internet is a part of everyday 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.

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 in the UTC is to raise educational standards, to promote pupil achievement, to support the professional work of staff 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.

2.2 How does internet use benefit education?

Provides access to worldwide educational resources including museums and art galleries;

Encourages inclusion in the National Education Network which connects all UK schools;

Allows educational and cultural exchanges between Students worldwide;

Provides access to experts in many fields for Students and staff;

Helps professional development for staff through access to national developments, educational materials and effective curriculum practice;

Helps collaboration across networks of schools, support services and professional associations;

Provides improved access to technical support including remote management of networks and automatic system updates;

Allows access to learning wherever and whenever convenient.

2.3 How can Internet use enhance learning?

The UTC’s Internet access will be designed to enhance and extend education.

Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

The UTC will ensure that the copying and subsequent use of Internet-derived materials by staff and Students complies with copyright law.

Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of students.

Staff should guide students to online activities that will support the learning outcomes planned for the students’ age and ability.

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 copyright when using Internet material in their own work.

2.4 How will students learn how to evaluate internet content?

The quality of information received via radio, newspaper and telephone is variable and everyone needs to develop critical skills in selection and evaluation. Information received via the internet, email or text message requires even better information handling and digital literacy skills. In particular it may be difficult to determine origin, intent and accuracy, as the contextual clues may be missing or difficult to read. A whole curriculum approach may be required.

Researching ethical issues in contemporary sciences will expose students to potentially emotive themes genetic modification, animal testing, nuclear energy etc providing an opportunity for students to develop skills in evaluating internet content.

Thus;

Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Students will use age-appropriate tools to research Internet content.

The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

3 MANAGEMENT INFORMATION SYSTEMS

3.1 How will information systems security be maintained?

It is important to review the security of the whole system from user to internet. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff and Students.

Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.

Users must take responsibility for their network use

Workstations should be secured against user mistakes and deliberate actions.

Servers must be located securely and physical access restricted.

The server operating system must be secured and kept up to date.

Virus protection for the whole network must be installed and current.

Access by wireless devices must be proactively managed and secured

The UTC’s Broadband network is protected by a cluster of high performance firewalls at the Internet connecting nodes in Liverpool. These industry leading appliances are monitored and maintained by a specialist security command centre.

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 used without specific permission

Unapproved software will not be allowed in work areas or attached to email.

Files held on the school’s network will be regularly checked.

The Director of ICT will review system capacity regularly.

The use of user logins and passwords to access the school network will be enforced.

3.2 How will email be managed?

Email is an essential means of communication for both staff and students. Directed email use can bring significant educational benefits; interesting projects between schools in neighbouring villages and in different continents can be created.

The implications of email use for the UTC and Students need to be thought through and appropriate safety measures put in place. Unregulated email can provide routes to Students that bypass the traditional school boundaries.

A central question is the degree of responsibility that can be delegated to individual Students as once email is available it is difficult to control. Restriction of incoming and outgoing email to approved addresses and filtering for unsuitable content is possible. In the school context (as in the business world), email should not be considered private and most schools and many firms reserve the right to monitor email. There is a balance to be achieved between necessary monitoring to maintain the safety of Students and staff and the preservation of human rights, both of which are covered by recent legislation. It is important that staff understand they should be using a work provided email account to communicate with parents/carers, Students and other professionals for any official UTC business. This is important for confidentiality and security and also to safeguard members of staff from allegations.

The use of email identities such as john.smith@lifesciencesutc.co.uk generally needs to be avoided, as revealing this information could potentially expose a child to identification by unsuitable people. Email accounts should not be provided which can be used to identify both a student's full name and their school.

When using external providers to provide students with email systems, close attention will be paid to the sites terms and conditions as some providers have restrictions of use and age limits for their services.

Spam, phishing and virus attachments can make email dangerous

Students may only use approved email accounts for school purposes.

Students must immediately tell a designated member of staff 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 an adult.

Staff will only use official UTC provided email accounts to communicate with Students and parents/carers, as approved by the Senior Leadership Team.

Access in school to external personal email accounts may be blocked.
Excessive social email use can interfere with learning and will be restricted.

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 would be.

The forwarding of chain messages is not permitted.

3.3 How will published content be managed?

Publication of any information online should always be considered from a personal and school security viewpoint. Material such as staff lists or a UTC plan may be better published in the UTC handbook or on a secure part of the website which requires authentication.

The contact details on the website should be the UTC address, email and telephone number. Staff or Students' personal information must not be published.

Email addresses will be published carefully online, to avoid being harvested for spam (e.g. by replacing '@' with 'AT'.)

The UTC website will comply with the UTC's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

3.4 Can Students' images or work be published?

The security of staff and Students is paramount. Although common in newspapers, the publishing of Students' names with their images is not acceptable. Published images could be reused, particularly if large images of individual Students are shown.

Personal photographs can be replaced with self-portraits or images of Students' work or of a team activity. Students in photographs should, of course, be appropriately clothed.

Students also need to be taught the reasons for caution in publishing personal information and images online.

Images or videos 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/videos of Students are electronically published.

Written consent will be kept by the UTC where Students' images are used for publicity purposes, until the image is no longer in use.

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

Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even very different interests. Users can be invited to view personal spaces and leave comments, over which there may be limited control.

For responsible adults, social networking sites provide easy to use, free facilities, although advertising often intrudes and some sites may be dubious in content. Students should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.

All staff should be made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They should be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

Examples of social media and personal publishing tools include: blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chatrooms, instant messenger and many others.

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.

Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom.

Staff official blogs or wikis should be password protected and run from the UTC website with approval from the Senior Leadership Team. Members of staff are advised not to run social network spaces for pupil use on a personal basis.

Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.

Students will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications.

Pupil will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.

All members of the UTC community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

Newsgroups will be blocked unless a specific use is approved.

Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.

Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the UTC Acceptable Use Policy.

3.6 How will filtering be managed?

Levels of Internet access and supervision will vary according to the pupil's age and experience.

Access profiles will be appropriate for all members of the UTC community. Older 6th form Students, as part of a supervised project, might need to access specific adult materials; for instance a course text or set novel might include references to sexuality.

Teachers might need to research areas including drugs, medical conditions, bullying, racism or harassment. In such cases, legitimate use should be recognised and restrictions removed temporarily. Systems to adapt the access profile to the pupil's age and maturity are available.

The UTC will work with Aimes and Lightspeed to ensure that filtering policy is continually reviewed.

The UTC will have a clear procedure for reporting breaches of filtering. All members of the UTC community (all staff and all Students) will be aware of this procedure.

If staff or Students discover unsuitable sites, the URL will be reported to the School Director of ICT who will then record the incident and escalate the concern as appropriate.

The UTC filtering system will block all sites on the Internet Watch Foundation (IWF) list.

Changes to the UTC filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.

The UTC Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective.

Any material that the UTC believes is illegal will be reported to appropriate agencies.

The UTC’s access strategy will be designed by educators to suit the age and curriculum requirements of the Students, with advice from network managers.

3.7 How will videoconferencing be managed?

Videoconferencing, including SKYPE, enables users to see and hear each other between different locations.

This ‘real time’ interactive technology has many uses in education.

Equipment ranges from small PC systems (web cameras) to large room-based systems that can be used for whole classes or lectures.

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 will not be made available to other sites.

Videoconferencing contact information will not be put on the UTC Website.

The equipment must be secure and if necessary locked away when not in use.

Academy videoconferencing equipment will not be taken off UTC premises without permission.

Responsibility for the use of the videoconferencing equipment outside school time will be established with care.

Users

Students will ask permission from a teacher before making or answering a videoconference call.

Videoconferencing will be supervised appropriately for the Students' age and ability.

Parents and carers consent should be obtained prior to children taking 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 videoconference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material shall be stored securely.

Videoconferencing 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.

3.8 How are emerging technologies managed?

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access, collaboration and multimedia tools.

A risk assessment needs to be undertaken on each new technology for effective and safe practice in classroom use to be developed. The safest approach is to deny access until a risk assessment has been completed and safety has been established.

Students will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the UTC Acceptable Use or Mobile Phone Policy.

3.9 How should personal data be protected?

The quantity and variety of data held on Students, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused.

The Data Protection Act 1998 (“the Act”) gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information.

Personal data will be recorded, processed, transferred and made available according to the UTC’s Data Protection Policy.

4. POLICY DECISIONS

4.1 How will Internet access be authorised?

The UTC will maintain a current record of all staff and Students who are granted access to the school’s electronic communications.

All staff will read and sign the UTC Acceptable Use Policy before using any UTC ICT resources.

Parents will be asked to read the UTC Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.

All visitors to the UTC site who require access to the schools network or internet access will be asked to read and sign an Acceptable Use Policy.

Parents will be informed that Students will be provided with supervised Internet access appropriate to their age and ability.

When considering access for vulnerable members of the UTC community (such as with children with special education needs) the UTC will make decisions based on the specific needs and understanding of the pupil(s).

4.2 How will risks be assessed?

The 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 school computer. The UTC cannot accept liability for the material accessed, or any consequences resulting from Internet use.

The UTC will audit ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Merseyside Police.

Methods to identify, assess and minimise risks will be reviewed regularly.

4.3 How will the school respond to any incidents of concern?

All members of the UTC community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).

The Director of ICT will record all reported incidents and actions taken in the **UTC** e-Safety incident log and other in any relevant areas e.g. Bullying or Child protection log.

The Designated Child Protection Coordinator will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.

The UTC will manage e-Safety incidents in accordance with the UTC discipline/ behaviour policy where appropriate.

The UTC will inform parents/carers of any incidents of concerns as and when required.

After any investigations are completed, the UTC will debrief, identify lessons learnt and implement any changes required.

Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguard Team or e-Safety officer and escalate the concern to the Police.

4.4 How will e–Safety complaints be handled?

Parents, teachers and Students should know how to use the UTC's complaints procedure. The facts of the incident or concern will need to be established and evidence should be gathered where possible and appropriate. e-Safety incidents may have an impact on Students, staff and the wider UTC community both on and off site and can have civil, legal and disciplinary consequences.

Complaints about Internet misuse will be dealt with under the UTC's complaints procedure.

Any complaint about staff misuse will be referred to the Vice Principal Curriculum.

All e–Safety complaints and incidents will be recorded by the UTC, including any actions taken.

Students and parents will be informed of the complaints procedure.

Parents and Students will need to work in partnership with the UTC to resolve issues.

All members of the UTC community will need to be aware of the importance of confidentiality and the need to follow the official UTC procedures for reporting concerns.

Any issues (including sanctions) will be dealt with according to the UTC's disciplinary, behaviour and child protection procedures.

All members of the UTC community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

4.5 How is the Internet used across the community?

Internet access is available in many situations in the local community. In addition to the home, access may be available at the local library, youth club, adult education centre, village hall, and supermarket or cyber café. Ideally, young people would encounter a consistent internet use policy wherever they are.

The UTC will liaise with local organisations to establish a common approach to e–Safety.

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

The UTC will provide appropriate levels of supervision for students who use the internet and technology whilst on the school site.

The UTC will provide an AUP for any guest who needs to access the school computer system or internet on site.

4.6 How will Cyberbullying be managed?

Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone.

Cyberbullying (along with all other forms of bullying) of any member of the UTC community will not be tolerated. Full details are set out in the UTC's policy on anti-bullying and behaviour.

There are clear procedures in place to support anyone in the UTC community affected by cyberbullying.

All incidents of cyberbullying reported to the 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.

The UTC will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

Students, staff and parents/carers will be required to work with the Academy to support the approach to cyberbullying and the school's e-Safety ethos.

Sanctions for those involved in cyberbullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
- Internet access may be suspended at the UTC for the user for a period of time. Other sanctions for Students and staff may also be used in accordance to the UTC's anti-bullying, behaviour policy or Acceptable Use Policy.
- Parent/carers of Students will be informed.
- The Police will be contacted if a criminal offence is suspected.

4.7 How will Learning Platforms be managed?

An effective learning platform or learning environment can offer UTC's a wide range of benefits to teachers, Students and parents, as well as support for management and administration. It can enable Students and teachers to collaborate in and across schools, sharing resources and tools for a range of topics. It also enables the creation and management of digital content and Students can develop online and secure e-portfolios to showcase examples of work.

SLT and staff will regularly monitor the usage of the LP by Students and staff in all areas, in particular message and communication tools and publishing facilities.

Students/staff will be advised about acceptable conduct and use when using the LP.

Only members of the current pupil, 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 the UTC their account or rights to specific school areas will be disabled or transferred to their new establishment.

Any concerns about content on the LP may be recorded and dealt with in the following ways:

a) The user will be asked to remove any material deemed to be inappropriate or offensive.
b) The material will be removed by the site administrator if the user does not comply.
c) Access to the LP for the user may be suspended.
d) The user will need to discuss the issues with a member of SLT before reinstatement.
e) A pupil's parent/carer may be informed.

A visitor may be invited onto the LP by a member of the 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 pupil to fulfil a specific aim and may have a limited time frame.

4.8 How will mobile phones and personal devices be managed?

Mobile phones and other personal devices such as Games Consoles, Tablets, PDAs and MP3 Players etc. are considered to be an everyday item in today's society and even children in early years settings may own and use personal devices to get online regularly. Mobile phones and other internet enabled personal devices can be used to communicate in a variety of ways with texting, camera phones and internet accesses all common features.

However, mobile phones can present a number of problems when not used appropriately:

- They are valuable items which may be stolen or damaged;
- Their use can render Students or staff subject to cyberbullying;
- Internet access on phones and personal devices can allow Students to bypass UTC security settings and filtering.
- They can undermine classroom discipline as they can be used on “silent” mode;
- Mobile phones with integrated cameras could lead to child protection, bullying and data protection issues with regard to inappropriate capture, use or distribution of images of Students or staff.

The use of mobile phones and other personal devices by students and staff in the UTC will be decided by the Principal and covered in the school Acceptable Use or Mobile Phone Policies.

The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the UTC community and any breaches will be dealt with as part of the UTC discipline/behaviour policy.

Academy staff may confiscate a phone or device if they believe it is being used to contravene the UTC behaviour or bullying policy. The phone or device might be searched by the Senior Leadership team with the consent of the pupil or parent/carer. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.

Mobile phones and personal devices will not be used during lessons or formal UTC time. They should be switched off at all times.

Mobile phones will not be used during lessons or formal UTC time unless as part of an approved and directed curriculum based activity with consent from a member of staff.

The Bluetooth function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.

Electronic devices of all kinds that are brought in to school are the responsibility of the user. The UTC accepts no responsibility for the loss, theft or damage of such items. Nor will the UTC accept responsibility for any adverse health effects caused by any such devices either potential or actual.

Mobile phones and personal devices are not permitted to be used in certain areas within the UTC site such as changing rooms, toilets and swimming pools.

Students Use of Personal Devices

- If a pupil breaches the UTC policy then the phone or device will be confiscated and will be held in a secure place in the UTC office. Mobile phones and devices will be released to parents/carers in accordance with the UTC policy.
- Phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- If a pupil needs to contact his/her parents/carers they will be allowed to use a UTC phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the UTC reception.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

Staff Use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- Staff will be issued with a UTC phone where contact with Students or parents/carers is required.
- Mobile Phone and devices will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by the Senior Leadership Team.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of Students and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.

5 COMMUNICATION OF THE POLICY

5.1 How will the policy be introduced to Students?

Many Students are very familiar with culture of mobile and Internet use and it is wise to involve them in designing the UTC e–Safety Policy, possibly through a student council. As Students' perceptions of the risks will vary; the e–Safety rules may need to be explained or discussed.

All users will be informed that network and Internet use will be monitored.

An e–Safety training programme will be established across the UTC to raise the awareness and importance of safe and responsible internet use amongst Students.

Pupil instruction regarding responsible and safe use will precede Internet access.

An e–Safety module will be included in the PSHE, Citizenship and/or ICT programmes covering both safe school and home use.

e–Safety training will be part of the transition programme across the Key Stages.

Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.

Particular attention to e-Safety education will be given where Students are considered to be vulnerable.

5.2 How will the policy be discussed with staff?

It is important that all staff feel confident to use new technologies in teaching and the UTC e–Safety Policy will only be effective if all staff subscribe to its values and methods.

Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies. It would be unreasonable, for instance, if cover or supply staff were asked to take charge of an Internet activity without preparation.

The e–Safety Policy will be formally provided to and discussed with all members of staff.

To protect all staff and Students, the school will implement Acceptable Use Policies. Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.

Staff who manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.

The UTC will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the Students.

All members of staff will be made aware that their online conduct out of UTC could have an impact on their role and reputation within the UTC. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

5.3 How will parents' support be enlisted?

Internet use in Students' homes is increasing rapidly, encouraged by low cost access and developments in mobile technology. Unless parents are aware of the dangers, Students may have unrestricted and unsupervised access to the Internet in the home. The UTC may be able to help parents plan appropriate, supervised use of the Internet at home and educate them about the risks. Parents should also be advised to check whether their child's use elsewhere in the community is covered by an appropriate use policy.

Parents' attention will be drawn to the school e–Safety Policy in newsletters, the UTC prospectus and on the UTC website.

A partnership approach to e-Safety at home and at UTC with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use, or highlighting e–Safety at other attended events e.g. parent evenings and sports days.

Parents will be requested to sign an e–Safety/Internet agreement as part of the Home School Agreement.

Parents will be encouraged to read the UTC Acceptable Use Policy for Students and discuss its implications with their children.

Information and guidance for parents on e–Safety will be made available to parents in a variety of formats.

Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents.

Interested parents will be referred to organisations listed in the "e–Safety Contacts and References section.

e-Safety Audit

This self-audit should be completed by the member of the Senior Leadership Team (SLT) responsible for e-safety policy. Staff that could contribute to the audit include: Designated Child Protection Coordinator, SENCO, e-Safety Coordinator, Network Manager and Head Teacher.

Has the school an e-Safety Policy	*Y/N*
Date of latest update:	
Date of future review:	
The UTC e-safety policy was agreed by governors on:	
The policy is available for staff to access at:	
The policy is available for parents/carers to access at:	
The responsible member of the Senior Leadership Team is:	
The governor responsible for e-Safety is:	
The Designated Child Protection Coordinator is:	
The Director of ICT is:	
Were all stakeholders (e.g. Students, staff and parents/carers) consulted with when updating the UTC e-Safety Policy?	*Y/N*
Has up-to-date e-safety training been provided for all members of staff? (not just teaching staff)	*Y/N*
Do all members of staff sign an Acceptable Use Policy on appointment?	
Are all staff made aware of the UTCs expectation around safe and professional online behaviour?	*Y/N*
Is there a clear procedure for staff, Students and parents/carer to follow when responding to or reporting an e-Safety incident of concern?	*Y/N*
Have e-safety materials from CEOP, Childnet and UKCCIS etc. been obtained?	*Y/N*
Is e-Safety training provided for all Students (appropriate to age and ability and across all Key Stages and curriculum areas)?	*Y/N*
Are e-safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all Students?	*Y/N*
Do parents/carers or Students sign an Acceptable Use Policy?	*Y/N*
Are staff, Students, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	*Y/N*
Has an ICT security audit been initiated by SLT?	*Y/N*
Is personal data collected, stored and used according to the principles of the Data Protection Act?	*Y/N*
Is Internet access provided by an approved educational Internet service provider which complies with DfE requirements?	*Y/N*
Has the school filtering been designed to reflect educational objectives and been approved by SLT?	*Y/N*

Are members of staff with responsibility for managing filtering, network access and monitoring systems adequately supervised by a member of SLT?	*Y/N*
Does the UTC log and record all e-Safety incidents, including any action taken?	*Y/N*
Are the Governing Body and SLT monitoring and evaluating the school e-Safety policy and ethos on a regular basis?	*Y/N*

e-Safety Contacts and References

CEOP *(Child Exploitation and Online Protection Centre):* *www.ceop.police.uk*

Childline: *www.childline.org.uk*

Childnet: *www.childnet.com*

Internet Watch Foundation *(IWF):* *www.iwf.org.uk*

Kidsmart: *www.kidsmart.org.uk*

Think U Know website: *www.thinkuknow.co.uk*

Virtual Global Taskforce *— Report Abuse:* *www.virtualglobaltaskforce.com*