Policy No: 23. Safeguarding – E-safety Policy

Coordinator	Executive Operations Manager
Review Frequency	Annually
Policy First Issued	2014
Last Reviewed	Autumn Term 2017
Date policy considered by External HR Consultant	N/A
Date policy considered by External Solicitor	N/A
Agreed by Governors and adopted on	17th November 2017
Does this policy need to be agreed by Governors? If yes, which committee	Yes, Board of Governors
Due for Review	Autumn Term 2018
This policy is communicated by the following means:	
Governors	Governor consultation by email when policy reviewed and agreement
Staff	Policy folders on staff shared drive and in-house training
Parents	Academy website, Parent Evenings
Students	Academy website, assemblies, in lessons

Safeguarding – E-safety Policy

Rationale

We recognise that protecting our staff and students properly means thinking beyond the traditional school environment. Our students of all ages have access to broadband connections through a variety of devices, and whilst network protection offers some safeguards **we aspire to educate all users so that they are aware** and understand the risks of electronic communications and act accordingly.

Consequently, e-safety is a matter of creating a safe ICT learning environment and is therefore a safety rather than an ICT issue. It is an extension of our policies on safeguarding.

The implementation and review of the e-safety policy is the responsibility of the Principal in liaison with the Designated Safeguarding Lead (DSL) and **all staff have responsibility for ensuring e-safety.**

1. Implementing the Policy - Roles and Responsibilities

Governors:

- Approve the policy and monitor its application

Principal and Senior Leadership Team:

- The Principal has a duty of care for ensuring the safety (including e-safety) of members of the school community.

- *The Senior Leadership Team will receive regular monitoring reports from the Designated Safeguarding Lead*

Network Manager / Technical staff will ensure that:

- the *school's* technical infrastructure is secure and is not open to misuse or malicious attack
- the *school* meets required e-safety technical requirements and any *East Sussex County Council* E-Safety Policy / Guidance that may apply.
- users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- *the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person*

- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the *network / internet / On-Line Learning Environment / remote access / email* is regularly monitored in order that any misuse / attempted misuse can be reported to the *Principal / Senior Leader; E-Safety Coordinator* for investigation
- *that monitoring software / systems are implemented and updated as agreed in school policies*

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy
- they report any suspected misuse or problem to the SLT
- they are aware of the risks posed by online activity of extremist and terrorist groups.
- all digital communications with students / parents / carers should be on a professional level and only carried out using official school systems

- e-safety issues are embedded in all aspects of the curriculum and other activities
- students understand and follow the e-safety and acceptable use policies
  - students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
  - they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
  - in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead will be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

2. Teaching and learning

2.1 The importance of Internet use

The purpose of Internet use at the UTC is to raise educational standards, to promote student independence in learning and achievement, to support the professional work of staff and to enhance the UTC's management functions.

Internet access is an entitlement for students who show a responsible and mature approach to its use. Sanctions will be used as appropriate for abuse of this entitlement in accordance with our Behaviour for Learning Policy.

Students use the Internet widely outside the UTC and we take responsibility in helping them learn how to evaluate Internet information and to take care of their own safety and security.

2.2 Using the Internet to enhance learning

ICT is a tool to enhance learning and to develop learning skills including the skills of knowledge location, retrieval and evaluation, networking and communication.

Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of students.

Staff should guide students in on-line activities that will support the learning outcomes planned for the students' age and maturity.

Students will be taught to evaluate the accuracy, relevance and suitability of internet material used in their learning.

3. Misuse and on-line bullying

Children and young people are open to the threat of increased bullying - known as online bullying, e-bullying or cyber-bullying. This form of bullying is defined as follows:

"The use of information and communication technologies to support deliberate, repeated, and hostile behaviour by an individual or group that is intended to harm others."

Bullying can take the form of:

- Text messaging
- Email
- Chat and Social Networking
- Instant Messaging

All report incidents of ICT misuse and cyber-bullying will be dealt with in accordance with our teaching and learning policies and our anti-bullying policy respectively.

4. Managing Information

4.1 Information system security

The security of the school information systems will be reviewed regularly but is the responsibility of all. All PCs, staff laptops must have UTC approved antivirus software which will be updated regularly.

Portable media may not used without specific permission followed by a virus check. Unapproved system utilities and executable files will not be allowed in students' work areas or attached to e-mail. The network manager will review system capacity regularly.

4.2 E-mail

The UTC will issue students with approved e-mail accounts which they may use for UTC work related communication. They can only be used for this purpose and other email accounts cannot be used for transferring files or communicating with UTC related matters.

Students must immediately tell a teacher if they receive offensive e-mail and must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission. The forwarding of chain letters is not permitted.

4.3 Management of published content

The contact details on the website should be the UTC's address, e-mail and telephone number. Staff or students' personal information must not be published. Staff school e-mail addresses will be published carefully. The Vice Principal (T&L) will take overall editorial responsibility and ensure that content is accurate and appropriate.

The website will comply with our guidelines for publications including respect for intellectual property rights and copyright. Training will be provided where appropriate.

4.4. Publishing of student images.

Written permission from parents or carers will be obtained before images of students are electronically published. Images that include students will be selected carefully and will not enable individual students to be clearly identified unless permission has been obtained from parents or carers.

Work can only be published with the permission of the student.

Student images captured on camera or by other means by staff can only be edited and processed at work or on work computers. No student images may be kept on file at home or a personal computer or other electronic storage device.

4.4 Management of social networking and personal publishing

The UTC will block/filter access to social networking site and newsgroups unless a specific use is approved. Students are advised never to give out personal details of any kind which may identify them and / or their location. Examples would include full name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.

Students are 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 e.g. House number, street name or school.

Teachers' official blogs or wikis should be password protected and run from the school website. Teachers may not to run social network spaces for student use on a personal basis.

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.

4.5 Web Filtering

The UTC will ensure that systems to protect students are reviewed and improved. Any potentially unsuitable sites must be reported to the SLT. He will manage the configuration of their filtering in consultation with our network management providers to ensure both educational and technical experience informs any decision. Any material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP.

4.6 Video conferencing.

Where practical, IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.

All videoconferencing equipment in the classroom must be switched off when not in use.

External IP addresses should not be made available to other sites.

Videoconferencing contact information should not be put on the school Website.

Students may engage in video conferencing under supervision once parental or guardian permission has been obtained. Students should ask permission from the supervising teacher before making or answering a videoconference call. Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure.

Staff organising a video conference should establish the parameters and content before taking part. They should ensure that written permission for student involvement has been obtained and are responsible for ensuring the conduct of the conference and that any recorded material is advised in advance, securely stored and is acceptable by all parties to avoid infringing property rights.

4.7 Emerging Technologies

The UTC will embrace the potential of emerging technologies for their application in learning and teaching. Emerging technologies will therefore be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Emphasis on all technologies will be on their appropriate use in lessons. Inappropriate use could result in confiscation.

4.8 Protection of personal data

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

5. Policy Decisions

5.1 Authorization to use the Internet

The UTC will maintain a current record of all staff and students who are granted access to the school's electronic communications. Use is only available to those who agree to the Acceptable Use Protocol.

5.2 Risk Assessment

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 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.

5.3 E-safety complaints procedure

Complaints of Internet misuse will be dealt with in the first instance by the class teacher, but referred to the Principal or DSL if the situation warrants it. The matter will be dealt with in accordance with our Behaviour for Learning Policy and may restrict or withdraw internet or other ICT access to individuals. A remedial action and timeframe must also be agreed at that point. Any complaint about staff misuse must be referred to the SLT.

6. Communicating the Policy

6.1 Policy introduction

Students will be informed that network and Internet use will be monitored. E-safety awareness is the responsibility of all staff, and students should have their attention drawn as appropriate to issues of e-safety and personal security and security of personal information. Staff will work with students to raise the awareness and importance of safe and responsible internet use. This will be done as appropriate through the planned curriculum. Instruction in responsible and safe use should precede Internet access. E-safety induction will form part of our Learning for life programme covering both school and home use.

6.2 Staff sharing of e-safety policy

All staff will be receive training in the UTC e-Safety Policy as part of the induction programme for all new staff. Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential. Staff training in safe and responsible Internet use and on the school e-Safety Policy will be provided as required.

6.3 Parental involvement

Parents' attention will be drawn to the school's e-Safety Policy in newsletters, the school brochure and on the UTC website. Internet issues will be handled sensitively, and parents will be advised accordingly. A partnership approach with parents will be encouraged. Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

Students will be made aware of the importance of filtering systems through the e-safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- signing the AUP
- induction training
- staff meetings, briefings, CPD.

Parents will be informed of the school's filtering policy through the Acceptable Use agreement and through e-safety awareness sessions / newsletter etc.

Changes to the Filtering System

- Staff may request a change to the UTC 's filtering system by email to the Network Manager
- Providing there is an educational reason for the change and guarantees are provided that changes to filtering will not be abused, permission will be granted. This could include access to You Tube or social networking sites. A decision will be made about who will be given access and whether this is a temporary change i.e. for a particular pieces of work. Any changes will be logged by the Network manager showing who has been given access, the period of access and the reasons for access being granted.
- The Network manager will check with the Senior Leader responsible for ICT before the final decision is made to allow access.
- The filtering log will be audited by the senior leader responsible for ICT once every half term.

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the Network Manager who will decide whether to make school level changes (as above).

Acceptable Use Policy Agreement

This Acceptable Use Policy is intended to ensure:

- That staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for *students / students* learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy/Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students / students receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, VLE etc) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident; I become aware of, to the appropriate person.

  I will be professional in my communications and actions when using school ICT systems:
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.

- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies. "Staff should not have students as 'online-friends' on social networking websites"
- I will only communicate with students / students and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the LA Personal Data Policy. Where personal data is transferred outside the secure school network, it must be encrypted.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date

Parent/Carer Acceptable Use Policy Agreement

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that *students / students* will have good access to ICT to enhance their learning and will, in return, expect the *students / students* to agree to be responsible users. A copy of the Student / Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent / Carers

Name Student / Pupil Name

As the parent / carer of the above *students / students*, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of ICT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Signed

Date