ICT ACCEPTABLE USE POLICY

Member of Staff Responsible	Deputy Principal
Board of Directors' Committee Responsible	Audit
Related policies	Behaviour management Anti-bullying Whistle blowing Safeguarding and Child Protection E-Safety Code of Conduct Disciplinary Procedures
Implementation date	28 February 2018
Review date	28 February 2020

Introduction

Silverstone UTC aspires to the highest standards of corporate behaviour to ensure that safe, fair and equitable procedures are applied to all organisational transactions, including relationships with staff, students and the use of public resources. In order to provide clear and consistent guidance, Silverstone UTC will develop documents to fulfil all statutory, organisational and best practice requirements and support the principles of equal opportunity for all.

Purpose and Scope

Silverstone UTC provide staff and students with an email facility, VLE, access to the Internet and an intranet which provides access to a wide range of UTC-specific information.

The purpose of the Acceptable Use Policy is to clearly identify for the whole school community:

- The steps taken in the UTC to ensure the Safety of pupils when using the internet, e-mail and related technologies.
- The UTC's expectations for the behaviour and the responsibilities of the whole community whilst using the internet, e-mail and related technologies within and beyond the UTC.
- The UTC's expectations for the behaviour of staff when accessing and using data.

The policy applies to:

- All staff employed by the UTC, students and trainees on temporary placements.
- Other individuals and agencies who may gain access to data, such as nonexecutive directors, volunteers, visiting professionals or researchers, and companies providing IT services to the UTC.

The policy should be used in conjunction with the UTC's disciplinary procedures and code of conduct applicable to employees and pupils. Where this policy is applied to the Principal, the Chair of Governors will be responsible for its implementation.

Legal Background

All adults who come into contact with children and young people in their work have a duty of care to safeguard and promote their welfare. The legal obligations and safeguarding duties of all UTC employees in relation to use of technologies feature within the following legislative documents which should be referred to for further information:

- The Children Act 2004.
- School Staffing (England) Regulations 2009.
- Working Together to Safeguard Children 2013.
- Education Act 2002.
- Keeping Children Safe in Education April 2014.
- Safeguarding Vulnerable Groups Act 2009.

Definitions -The following terms are used in this document:
Intranet: The intranet is a website that is internal to UTC staff and students and provides access to a wide range of UTC-specific information.
Spamming - Spam is unsolicited commercial email, the electronic equivalent of the junk mail that comes through your letterbox.
Phishing - Phishing is the use of bogus emails and websites to trick an email user into supplying confidential and personal information.
Chain Letters - A chain letter is an electronic email that urges you to forward copies to other people.
Virus - A computer virus is a computer program that can copy itself and infect a computer.
Internet: A worldwide system of interconnected networks and computers.
VLE: or **learning platform**, is an e-learning education system based on the web that models conventional in-person education by providing equivalent virtual access to classes, class content, tests, homework, grades, assessments, and other external resources such as academic or museum website links. It is also a social space where students and teacher can interact through threaded discussions or chat.

Policy Details

- Email and the internet are fast and effective electronic means of communicating and gathering information that can enhance the efficiency and effectiveness of staff and students in the UTC.
- The facilities exist primarily for the purpose of conducting UTC business but can also be used for permitted personal purposes.
- Email carries the same legal status as other written documents and should be used with the same care.
- Email allows electronic records of communications over a period of time to be maintained and systematically managed and referenced.
- The Internet provides a wide-ranging source of information and knowledge but offers no guarantee of accuracy, reliability and authenticity.
- The UTC will use these facilities to the full (but within available resources and technology) in communicating and cascading information throughout the organisation. Staff are encouraged to familiarise themselves with the facilities and to make use of the VLE site.
- The email and internet facilities employ complex technology which is not 100% reliable and staff should not rely wholly and solely on them for critical business processes.
- Staff email accounts are created and hosted on Microsoft's Edu Mail platform, this is a specific educational version of email, similar to Hotmail. This is available via the internet 24/7 365 days of the year.

- Student email accounts are created and hosted on Microsoft's Edu Mail platform, this is a specific educational version of email, similar to Hotmail. This is available via the internet 24/7 365 days of the year.

Core Principles

- All Staff and students will have access to e-mail, the intranet, VLE and the Internet.
- Recognised and authorised third party organisations, will have access to e-mail and the Internet.
- Personal use of the facilities will be limited and within prescribed areas; Safeguards will be established to protect the security, integrity and availability of the UTC's systems.
- The requirements of relevant Acts of Parliament and mandatory national policies will be observed at all times. Computer Misuse Act 1990, Data Protection Act 1998, Privacy and Electronic Communications (EC Directive) Regulations 2003.
- Staff awareness of copyright and contractual issues will be raised.
- Guidance on e-mail etiquette will be observed, (see section 3.3)
- Guidance on housekeeping to ensure efficiency in the operation of the network and personal folders will be observed, (see section 3.3 housekeeping and general responsibilities).

Common Standards – Email

As more attached documents are carried with email the potential for spreading of computer viruses is greatly increased. It is important to realise that viruses can be carried by documents and as soon as you open the infected attached document the virus will infect your system. A potentially greater risk is sending viruses out of the organisation and infecting other organisations, as such occurrences could result in legal action against the UTC. All staff and students using email must have an up to date antivirus scanner capable of scanning email attachments. As with all communication systems there is a potential security risk as to who has access to the information, you should not allow others to read your email unless you intentionally forward it to them. There is also the danger that received email messages may be forwarded to other people not authorised to handle sensitive material. Highly sensitive messages should not be sent by email. For sensitive messages the sender should check with the intended recipient that the information will go directly to him/her and will not be passed on to anyone else. All emails will automatically contain a confidentiality notice when sent externally asking to be informed if the incorrect person receives the e-mail, such as:

"This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please destroy it and notify the sender."

Email is often perceived as an informal medium. However emails occupy the same place legally as letters - it is just like writing on company headed notepaper - therefore care must be taken to prevent:

- Inadvertently entering into contracts through email committing libel.
- Using inappropriate language or graphics, this may be construed as sexual harassment or an offence under the Race Relations Act.
- Breach of copyright by "publication" of original material even by forwarding to another individual.

Access – Email is available to all staff and students who are registered as users of the computer network. All users are required to complete a 'User Code of Connection' form which needs to be authorised by their Tutor and submitted to IT Services before access is granted. A copy of this form can be found at *Appendix*

A. This form must be signed by the individual. The signature can be digital, or where a paper version of the form is used it should be scanned and emailed/faxed, or sent via the internal post system.

Personal Use – Although personal use of e-mail facilities is discouraged, *limited* personal use will be permitted provided that the content of messages is appropriate, i.e. is not likely to cause offence. Staff and students should regard this facility as a privilege that should normally be exercised in their own time without detriment to the job or study and not abused. Inappropriate or excessive use may result in disciplinary action and/or removal of facilities. However, staff should be aware that both private and business use of e-mail will be subject to monitoring.

Accessing the Mailbox of another Member of Staff – There may be occasions when it is necessary to access email messages from an individual's mailbox when a person is away from the office for an extended period, for example sick leave. The reasons for accessing an individual's mailbox are to action:

- Subject access request under the Data Protection Act.
- Freedom of Information requests.
- Evidence in legal proceedings.
- Line of business enquiry.
- Conducting an investigation which may result in disciplinary action.
- Where it is not possible to ask the permission of the member of staff whose mailbox needs to be accessed, the procedure for gaining access to their mailbox is:

  Authorisation is given by a member of the Leadership team who will forward a request to the IT Service Desk authorising access to the mailbox. A record will be made of the reason for accessing the mailbox together with the names of the people involved and the person whose mailbox was accessed will be informed.

Housekeeping – The amount of e-mail in the personal Inbox should be kept to a minimum. E-mails should be deleted after reading, response, or action. Saved emails should be reviewed on a monthly basis and deleted when no longer required.

E-mails that need to be saved should be moved to a personal folder. The same housekeeping rules apply to sent items. Care should be taken when sending file attachments as these are typically large and may cause network congestion. File attachments should only be sent when necessary and should be deleted as soon as is practicable.

General responsibilities – Staff and students should adhere to the following guidelines:

- For a secure permanent record, emails should be printed out and filed like any other correspondence.
- You must not use the email service to violate any laws or regulations of the United Kingdom or other countries. Use of the service for illegal activity is usually grounds for immediate dismissal and any illegal activity will be reported to the police. Illegal activity includes, but is not limited to, sending or receiving material related to paedophilia, terrorism, incitement to racial harassment, stalking and sexual harassment and treason. Use of the service for illegal activity will result in the immediate suspension of your email account.
- You must not use the email service for personal commercial gain. This includes, but is not limited to: marketing, advertising and selling goods or services.
- You must not attempt to interfere with the technical components, both hardware and software, of the email system in any way.

- You must ensure your password and any answers to your security questions for the email system are kept confidential and secure at all times.
- You must not use the email service to disable or overload any computer system or network.

Responsibilities when using email service – Staff should adhere to the following guidelines:

- You must not attempt to disguise your identity or your sending address.
- You must not send any material by email that could cause distress or offence to another user. You must not send any material that is obscene, sexually explicit or pornographic.
- You must not forward chain emails or other frivolous material.
- It is your responsibility to check that you are sending email to the right recipient, as there may be more than one person with the same name.
- Always check that you have the correct email address for the person you wish to send to - this can be done by checking their entry in the Global Directory
- Email is admissible as evidence in a court of law and messages are classified as legal documents. Internal emails may also need to be disclosed under the Freedom of Information Act 2000. Emails should be treated like any other communication and care should be taken to ensure that content is accurate and the tone is appropriate.

Harassment – It is strictly forbidden to send messages that contain offensive or harassing statements or language, particularly in respect of race, national origin, sex, sexual orientation, age, disability, religious or political beliefs. Remarks sent by e-mail that are capable of amounting to harassment may lead to complaints of discrimination under the Sex or Disability Discrimination Acts, or the Race Relations Act.

Defamation – The ease of use of e-mail can lead to unguarded and impetuous comments being made, which in turn could be classified as defamatory. Defamation arises where there is the publication of an untrue statement tending to lower the subject of the statement (which may be an individual or an organisation) in the estimation of the public generally. Liability for the tort of defamation applies to electronic communication just as it does to more traditional forms of publishing.
Staff and students are therefore advised to take care when drafting e-mails to ensure that the content is not libellous.

Copyright – Under the Copyright, Designs and Patents Act 1988, copyright law can be infringed by making an electronic copy or making a 'transient' copy (which occurs when sending an e-mail). Copyright infringement is becoming more commonplace as more and more people forward text, graphics, audio and video clips by e-mail. Staff and students must not, therefore, copy, forward, or otherwise disseminate third-party work without appropriate consent.

Viruses – Viruses can damage computer systems, destroy data, cause disruption and incur considerable expense for the UTC. Staff and students connected to the network must ensure that they have an appropriate virus scanner on their PC and that this is regularly updated (IT Services will ensure this is the case). Staff and students must not open attachments from external sources without first checking for viruses using the virus scanner installed by the IT Services (usually this is carried automatically by the anti-virus software). If any viruses are found, the IT Security Officer and/or the IT Service Desk must be informed immediately. The downloading and subsequent use of any software received via e-mail, without the prior approval of IT Services, is strictly forbidden (this includes screen savers).

Hoaxes, Scams & Chain Letters – If you receive any form of these emails do not forward them to anyone, delete them immediately.

Unsolicited Email (spamming) – IT Services and Microsoft Edu Mail carry out various levels of checks on inbound and outbound email to try and ensure that the level of unsolicited email you receive is low. Users can set up filters both of which can prevent unsolicited mail.

"SPAM" Mail can be avoided by the following:

- If you don't know the sender, delete the email.
- Never respond to spam or click on links within it.
- Never give your email address on the internet.
- Only give your email address to people you trust.
- Use the 'bcc' field if you email many people at once.
- Never make a purchase from unsolicited email.

Etiquette – Staff should adhere to the following guidelines:

- All e-mail messages should be written in lower case as using CAPITAL letters is considered to be aggressive.
- The subject field should always be used to add a short description of the contents of the e-mail. This will assist the recipient in prioritising opening of e-mail and aids future retrieval of opened messages.
- Care should be taken with content. Nothing should be written in an e-mail that would not be written in a letter or said to someone face to face.
- The same conventions should be used as when sending a letter by post, e.g. using the same style of salutation.
- Emails should be signed off with the name, title and contact details of the sender.
- Read the email before you send it. Think if your first reaction is the one you want the recipient to receive. If you are unsure, save it in the Draft box and edit it later before sending to ensure that it conveys the correct message.
- Make proper arrangements about how your e-mail will be handled when you are away; set up a suitable auto reply.
- Avoid the overuse of 'Reply to All'. Only reply to those who need to know your response, i.e. not everyone needs to know that you will not be attending a meeting. A method to use to avoid replies being sent to all is when sending emails to group addresses (such as UTCaddresss@ac.uk etc.), put the group address in the 'Bcc:' field and the sender's address in the 'To:' field. This means any replies will come back to the sender and avoids replies being sent to all addresses.

Formation of Contracts – E-mail is capable of forming or varying a contract in just the same way as a written letter. Such capability gives rise to the danger of staff inadvertently forming contracts on behalf of the UTC or varying contractual terms to which the UTC then becomes bound. Staff should take due care when drafting the words of an e-mail so that they cannot be construed as forming or varying a contract when this is not the intention.

Common Standards – Internet

Access - All users are required to complete a 'User Code of Connection form which needs to be submitted to IT Services before access is granted. A copy of this form can be found at *Appendix A*. This form must be signed by the individual.

Personal Use – Limited personal use of Internet facilities is permitted provided that the material accessed is appropriate and is not potentially offensive to others. The use of the Internet for personal transactions only, such as booking reservations or tickets or the purchase of any goods or services for personal use, is permitted.
Staff should regard this facility as a privilege that should not be abused and should normally be exercised in their own time and without detriment to the job. Inappropriate or excessive use may result in disciplinary action and/or removal of facilities. Staff and students should be aware that Internet access will be subject to monitoring.

Inappropriate Use – Access to websites that contain inappropriate material will be blocked, e.g. pornography, instruction on criminal or terrorist skills, promotion of cults, gambling, content or statements of a nature which are liable to cause offence to others, or any other material likely to bring the UTC into disrepute. It is understood that access to subjects and sites of a potentially contentious nature may be appropriate in some areas of normal operation and/or in specific circumstances, e.g. sex education, youth advice, counselling, approved research, etc. The UTC therefore places special responsibilities of care on staff operating in such areas to ensure that such access is necessary and that other staff and students are not exposed to any such material without good cause. Any requests for such sites should be placed with the IT Security officer. Staff should not use the Internet to conduct personal transactions in pursuit of their own commercial or business interests nor in such a way as to implicate the UTC in those transactions. If in doubt, staff should consult the IT Security Officer.

Copyright – Files must not be downloaded from the Internet and used in such a way as to violate copyright laws. Even if downloading is permissible under copyright law, there may be restrictions with regard to copying, forwarding, or otherwise distributing files. Software license agreements should be read and adhered to. Staff and students must not transmit copyright software from their computer via the Internet.

Viruses – Viruses can damage computer systems, destroy data, cause disruption and incur considerable expense for the UTC. Staff and students connected to the network must ensure that they have an appropriate virus scanner on their PC and that this is regularly updated (IT Services will ensure this is the case). Staff and students must not open attachments from external sources without first checking for viruses using the virus scanner installed by the IT Services (usually this is carried automatically by the anti-virus software). If any viruses are found, the IT Security Officer and/or the IT Service Desk must be informed immediately. The downloading and subsequent use of any software received via e-mail, without the prior approval of IT Services, is strictly forbidden (this includes screen savers).

Accuracy – Information obtained through the Internet may not be accurate, and users must check the accuracy, adequacy or completeness of any such information.

Internet Service Providers – Individuals must not independently arrange Internet access of any nature (neither dial-up nor leased line) direct with a commercial Internet Service Provider.

Duties and Responsibilities

Board of Directors

The Board of Directors of Silverstone UTC have responsibility for the strategic context in which organisational process documents are developed, and for establishing a scheme of governance for the formal review and approval of such documents.
The Board of Directors of Silverstone UTC have overall responsibility for the strategic direction and operational management, including ensuring that UTC process documents comply with all legal, statutory and good practice guidance requirements.

The Board of Directors is responsible for ensuring that:

- The document is drafted, approved and disseminated in accordance with the Policy for the Development and Approval of Policies.
- The necessary training or education needs and methods required to implement this policy are identified and resourced or built into the delivery planning process.
- Mechanisms are in place for the regular evaluation of the implementation and effectiveness of this policy.

Head of IT Services working with the Senior team of the UTC

The IT Support Services Manager with the UTC Senior team will:

- Review the policy
- Update the policy

All Staff

All staff, including temporary and agency staff, are responsible for:

- Compliance with relevant process documents. Failure to comply may result in disciplinary action being taken.
- Co-operating with the development and implementation of policies and procedures and as part of their normal duties and responsibilities.
- Identifying the need for a change in policy or procedure as a result of becoming aware of changes in practice, changes to statutory requirements, revised professional standards and local/national directives, and advising their line manager accordingly.
- Identifying training needs in respect of policies and procedures and bringing them to the attention of their line manager.
- Attending training / awareness sessions when provided.
- Reporting known or suspected misuse of the ICT systems that is believed to be illegal, inappropriate or abusive to the Designated Senior Person for Safeguarding.

Examples of inappropriate use:

- Accepting or requesting pupils as 'friends' or otherwise connecting on social networking sites, or exchanging personal email addresses or mobile phone numbers with students.
- Behaving in a manner online which would lead any reasonable person to question an individual's suitability to work with children or act as a role model.

Implementation

This policy will be available to all Staff and Students:

- The Senior Leaders and staff are responsible for ensuring that relevant staff and students within their own schools and service departments have read and understood this document and are competent to carry out their duties in accordance with the procedures described. It may be necessary to develop specific implementation plans.

Training Implications

The senior leadership team will ensure that the necessary training or education needs and methods required to implement the policy or procedure(s) are identified and resourced or built into the delivery planning process. This may include identification of external training providers or development of an internal training process. Silverstone UTC shall ensure that its staff, contractors and agents are aware of its policies and requirements regarding INTERNET, VLE, INTRANET and E-MAIL and appropriate training arrangements will be made available, bearing in mind the number and turnover of staff and students concerned.

Legislation and statutory requirements

Cabinet Office. (1998) *Data Protection Act 1998*. London: HMSO
Cabinet Office. (1998) *Human Rights Act 1998*. London: HMSO
Cabinet Office. (1990) *The Computer Misuse Act 1990*. London: HMSO
Cabinet Office. (2000) *The Electronic Communications Act 2000*. London: HMSO
Privacy and Electronic Communications (EC Directive) Regulations 2003

Useful Links

NASUWT Social Networking- Guidelines for Members
http://www.nasuwt.org.uk/InformationandAdvice/Professionalissues/SocialNetworking

NUT E-Safety: Protecting School Staff- Guidance for Members http://www.teachers.org.uk/node/12516

Appendix A: User Code of Connection, including Access to Internet, VLE and Email Services.

Introduction

This code of connection provides a key summary of pertinent information contained within the ICT Acceptable Use Policy. Signing the User Code of Connection Agreement means you agree to this summary and to the policy in full.

Key Summary – User Code of Connection

- Internet and email services are provided for those purposes directly related to a user's work/study and/or areas of legitimate research.
- Limited personal use of the services is permitted.
- Care must be taken to ensure only the intended recipients have access to email messages.
- Emails should be saved to storage medium to prevent loss.
- You must not divulge your logon details including password to anyone.
- Passwords must be changed a minimum of every 90 days and must adhere to the password policy as set out in the IT Security Guide.
- No illicit material will be sent/viewed/downloaded or obtained via the UTC systems, advice should be taken where there is any doubt.
- An up to date antivirus product must be installed on equipment that is to be connected to the UTC network. All UTC IT equipment will have up to date antivirus software on by default.
- Unlicensed or unauthorised software must not be installed on any UTC PC.
- The user will not make use of third party software (e.g. proxy servers) on personal devices to override the firewall set up on the UTC Wi-Fi network.
- Modems/ADSL/External Wi-Fi must not be connected to PC's on the UTC network.
- Limited personal data can be stored on personal network drives and where permitted on SUTC local laptop hard drives. However mass storage of personal photos, music etc. is not permitted and may be deleted from the Silverstone UTC system.
- Data quotas may be enforced if appropriate to manage the UTC's data storage requirements, to ensure data integrity, backup integrity and storage costs.
- Email quotas may be enforced if appropriate to manage the UTC's email storage requirements, to ensure email integrity, backup integrity and storage costs.
- All copyright restrictions must be adhered to.
- Breaches of security, abuse of services or non-compliance with the UTC's IT Security Policy, Internet, Intranet and Email Acceptable Use Policy or the Code of Connection, may result in the withdrawal of services and further action.
- The UTC's disciplinary procedures will be invoked should abuse of services or non-compliance occur.
- **Note: The UTC reserves the right to monitor systems, including internet access and emails sent or received on UTC equipment, in order to ensure that the Code of Connection is not breached.**

USER ACCEPTANCE AGREEMENT

I have read and understand the User Code of Connection and agree to abide by it.

User Signature: .....

Name (please print): .....

Telephone: ..... Date: .....

School: .....