E-safety and Acceptable Use Policy

Produced: April 2017
To be presented to Project Steering Group: June 2017
Review: April 2018

1. Introduction

The Mulberry UTC E-safety and Acceptable Use Policy is to prevent unauthorised access and other unlawful activities by users online. As used in this policy, "user" includes anyone using the computers (network), internet, email and other forms of direct electronic communications or equipment provided by the Mulberry UTC. It also covers any outside equipment that uses the school network to access the internet.

Only current students or employees are authorised to use the network. Other users, such as governors and guests, can be authorised by the Principal.

Mulberry UTC will use technology protection measures to block or filter, to the extent possible, access of verbal and visual depictions that are obscene, pornographic, violent and harmful to pupils and other users over the network. The school reserves the right to investigate users' online activities and to access, review, copy, and store or delete any electronic communication or files and disclose them to others as it deems necessary. Users should have no expectation of privacy regarding their use of school's network and/or internet access or files, including email.

2. Acceptable Uses of the School's Computer Network and the Internet

All pupils are inducted into to the acceptable use policy when they join the UTC. Pupils and their parents/carers must sign the AUP and the school must keep the signed page on file.

2.1 Staff Internet Use

Employees and other users are required to follow this policy. Even without a signature, all users must follow this policy and report any misuse of the network or internet by pupils to a teacher, supervisor or other appropriate school staff. Access is provided primarily for educational purposes. Staff may use the internet for incidental personal use during duty-free time.

2.2 Unacceptable Uses of the Computer Network or Internet

The following are examples of inappropriate activity on the internet/intranet and school's website. The UTC reserves the right to take immediate action regarding any activities that create security and/or safety issues for the school, students, employees, school's network or computer resources, including but not limited to the following:

- Violating any law such as: accessing or transmitting any kind, obscene, harmful materials, materials that encourage others to violate the law, confidential information or copyrighted materials;
- Criminal activities that can be punished under law
- Selling or purchasing illegal items or substances
- Obtaining and/or using anonymous email sites; spamming; spreading viruses
- Causing harm to others or damage to their property, such as;
    - Using abusive, or impolite language; threatening, harassing, or making damaging or false statements about others or accessing, transmitting, or downloading offensive, harassing materials;
    - Deleting, copying, modifying, or forging other users' names, emails, files, or data; disguising one's identity, impersonating other users, or sending anonymous email;
    - Damaging computer equipment, files, data or the network in any way, including intentionally accessing, transmitting or downloading computer viruses or other harmful files or programs, or disrupting any computer system performance;

- Using any school computer to pursue "hacking," internal or external to the school, or attempting to access information protected by privacy laws; or
- Accessing, transmitting or downloading "chain letters"
- Using another's account password(s) and user identifier(s);
- Disclosing anyone's password to others or allowing them to use another's account(s)
- Using the internet for personal financial gain
- Using the internet for personal advertising, promotion, or financial gain

3. Student Internet Safety

Students under the age of eighteen should only access Mulberry School accounts outside of school if a parent or legal guardian supervises their usage at all times. The student's parent or guardian is responsible for monitoring the minor's use;

Students shall not reveal on the internet personal information about themselves or other persons. For example, students should not reveal their name, home address, telephone number, or display photographs of themselves or others;

Students shall not meet in person anyone they have met only on the internet;

The use of a school account is a privilege, not a right, and misuse will result in the restriction or cancellation of the account. Misuse may also lead to disciplinary action for students.

4. Social Networking & Instant Messaging (IM) Policy

Mulberry UTC staff and students are prohibited from using social media (e.g. Twitter, Snapchat, Instagram) or personal instant messaging (e.g. Facebook messenger) on school computers or other devices, or using the wireless internet connection provided by the UTC. The only exception is when permission is given explicitly by the Principal, e.g. for social media platforms which are used for marketing purposes for the UTC.

When using social media or instant messaging services, students and staff should refrain from causing harm to others and must ensure that language used in any online communications is appropriate and non-offensive. Staff and students are specifically prohibited from transmitting anything that includes abusive or impolite language, threatening, harassing, or making damaging or false statements about others or accessing, or transmitting offensive, harassing materials.

5. Email Policy

5.1 Introduction

Mulberry UTC provides students, teachers and staff with electronic communications tools including an email account. This acceptable use policy governs use of Mulberry UTC's email system and applies to email use in school sites, as well as at remote locations including but not limited to staff or students' homes or other locations.

5.2 Scope of email use

Email and the internet can be extremely valuable tools in an educational context, encouraging the development of communication skills, and transforming the learning process by opening up possibilities that, conventionally, would be impossible to achieve. Mulberry UTC encourages the use of electronic mail as a medium for paper mail replacement and as a means of enhancing communications.

Mulberry UTC follows sound professional practices to secure email records, data and system programmes under its control. As with standard paper-based mail systems, confidentiality of email cannot be 100% assured. Consequently, users should consider the risks when transmitting highly confidential or sensitive information and use the appropriate level of security measure.

Enhancement of the base level security to a higher or intermediate level can be achieved by the use of passwords for confidential files. It should be remembered emails forwarded from another individual can be amended by the forwarder. This possibility should be considered before acting on any such mail.

Only current students or employees (or guests authorised by the Principal) are authorised to use the school email. The UTC reserves the right to investigate users' email activities and to access, review, copy, and store or delete any electronic communication or files and disclose them to others as it deems necessary. Users should have no expectation of privacy regarding their use of school email.

In order to effectively manage the email system, the following should be adhered to:

- Open mailboxes must not be left unattended.
- Care should be taken about the content of an email as it has the same standing as a memo or letter. Both the individual who sent the message and/or Mulberry UTC can be sued for libel.
- Reporting immediately to IT staff when a virus is suspected in an email.

5.3 Privacy

There should be no expectation of privacy. Email messages created and transmitted on Mulberry UTC computers are the property of Mulberry UTC and users have no right to expect that their emails may not be inspected as it deems necessary. The UTC reserves the right to investigate if necessary all email transmitted via the school computer systems. Students and staff have no reasonable expectation of privacy when it comes to school and personal use of the school's email system.

Mulberry UTC respects users' privacy. Email content will not be routinely inspected or monitored, nor content disclosed without the originator's consent. However, under the following circumstances such action may be required:

- When required by law.

- If there is a substantiated reason to believe that a breach of the law or Mulberry UTC policy has taken place.
- When there is an emergency or compelling circumstances.

Mulberry UTC reserves the right, at its discretion, to review any employee's electronic files and messages to the extent necessary to ensure electronic media and services are being used in compliance with the law, this policy and other Mulberry UTC policies.

An employee should not have any expectation of privacy to his or her internet usage. Mulberry UTC reserves the right to inspect freely any and all files stored in computers or on the network in order to assure compliance with this policy. Auditors must be given the right of access to any document, information or explanation that they require.

Use of the employee's designated personal file area on the network server provides some level of privacy in that it is not readily accessible by other members of staff. These file areas will however be monitored to ensure adherence to Mulberry UTC's policies and to the law. The employee's personal file area is disk space on the central computer allocated to that particular employee. Because it is not readily accessible to colleagues it should not be used for the storage of documents or other data that should be open and available in Mulberry UTC.

Managers will not routinely have access to an employee's personal file area. However, usage statistics/management information on usage size of drives or a report outlining the amount of information held on an individual's personal file area will be made available from time to time.

5.4 Unacceptable uses of school email

The following are examples of inappropriate use of school email. The UTC reserves the right to take immediate action regarding the following activities:

- Any activities that create security and/or safety issues for the UTC, students, employees, school's network or computer resources.
- Other activities as determined by the UTC as inappropriate; such as: Transmitting pornography of any kind, obscene depiction and harmful materials, materials that encourage others to violate the law, confidential information or copyrighted materials.
- Engaging in uses that jeopardise access or lead to unauthorised access into others' email accounts such as: Using another's account password(s) or username(s), disclosing anyone's password to others. or allowing them to use another's account(s)
- Using school email for commercial purposes.
- Using school email for personal financial gain.
- Using school email for personal advertising, promotion, or financial gain.
- Solicitation for religious purposes or lobbying for personal political purposes.
- Obtaining and/or using anonymous email sites; spamming; spreading viruses.
- Using abusive or impolite language; threatening, harassing, or making damaging or false statements about others; accessing, or transmitting offensive, harassing materials; deleting, copying, modifying, or forging other users' names, emails, files, or data; disguising one's identity, impersonating other users, or sending anonymous email; accessing, transmitting or downloading large files, including "chain letters" or any type of "pyramid schemes".

The use of a school email account is a privilege, not a right, and misuse will result in the restriction or cancellation of the account. Misuse may also lead to disciplinary and/or legal action for both students and employees.

5.5 Usage at home

Access to the internet from an employee's home using a Mulberry UTC-owned computer or through Mulberry UTC-owned connections must adhere to all the policies that apply to use within Mulberry UTC. Mulberry UTC employees may use email to communicate with spouses, children, domestic partners, and other family members. Family members or other non-employees must not be allowed to access Mulberry UTC's computer system or to use Mulberry UTC's computer facilities, without the formal agreement of the Principal.

5.6 Email protocols

Users must **not**:

- Routinely ignore emails. The system is designed for speedy communication. If a message requires a reply, a response should be sent as promptly as possible.
- Use anonymous mailing services to conceal identity when mailing through the internet, falsify emails to make them appear to originate from someone else, or provide false information to any internet service which requests name, e-mail address or other details.
- Abuse others (known as 'flaming'), even in response to abuse directed at themselves.
- Use electronic media and services in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system.
- Use email, either internally or on the internet, to sexually harass fellow employees, or harass or threaten anyone in any manner.
- Use, transfer or tamper with other people's accounts and files.
- Disrespect copyrights and copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner.
- Use the internet/intranet facilities or equipment to deliberately propagate any virus, worm, Trojan horse or any such other programme that is harmful to normal computer operations.
- Access any obscene or pornographic sites. Sexually explicit or other offensive material may not be viewed, archived, stored, distributed, edited or recorded using Mulberry UTC's networks or computing resources. If a user finds himself/herself connected accidentally to a site that contains sexually explicit or offensive material, s/he must disconnect from that site immediately. Such unintentional access to inappropriate internet sites must be reported immediately to the respective line manager or Principal. Any failure to report such access may result in disciplinary action.

Except in cases in which explicit authorisation has been granted at an appropriate level of Mulberry UTC management, employees are prohibited from engaging in or attempting to engage in:

- Monitoring or intercepting the files or electronic communications of other employees or third parties.
- Hacking or obtaining access to systems or accounts they are not authorised to use.
- Using other people's log-ins or passwords.
- Breaching, testing, or monitoring computer or network security measures.
- Email or other electronic communication that attempts to hide the identity of the sender or represent the sender as someone else.

- Interfering with other people's work or computing facilities.
- Sending mass emails without consultation with the Principal. Global Sends (sending emails to everybody in the address book) are prohibited.
- Using the internet for personal commercial purposes.

5.7 The law

The Data Protection Act 1998 prohibits the disclosure of personal data except in accordance with the principles of the Act. This prohibition applies to e-mail in the same way as to other media. Information gathered on the basis that it would be seen by specified employees must not be given to a wider audience. In accordance with the provisions of Article 8 of the European Convention on Human Rights, Mulberry UTC respects the right to privacy for employees who use IT equipment but does not offer any guarantee of privacy to employees using IT equipment for private purposes.

As a data controller, Mulberry UTC has responsibility for any data processed or stored on any of its equipment. Any employee monitoring will be carried out in accordance with the principles contained in the Code of Practice issued by the Information Commissioner under the provisions of the Data Protection Act 1998.

In order to comply with its duties under the Human Rights Act 1998, Mulberry UTC is required to show that it has acted proportionately, i.e. it is not going beyond what is necessary to deal with the abuse and that the need to investigate outweighs the individual's rights to privacy, taking into account Mulberry UTC's wider business interests. In drawing up and operating this policy Mulberry UTC recognises that the need for any monitoring must be reasonable and proportionate.

Auditors (internal or external) are able to monitor the use of Mulberry UTC's IT equipment and the storage of data. They are nevertheless bound by the provisions of the Human Rights Act 1998, the Data Protection Act 1998, associated codes of practice and other statutory provisions and guidance, including the Regulation of Investigatory Powers Act 2000 in respect of any activity that could be classed as directed surveillance.

Specific Legislation

- **The Human Rights Act 1998** provides for the concept of privacy giving, a 'right to respect for private and family life, home and correspondence'.

- **The Regulation of Investigatory Powers Act 2000** covers the extent to which organisations can monitor or record communications at the point at which they enter or are being sent within the employer's telecommunications system.

- **The Data Protection Act 1998**. Codes of Practice clarify the Act in relation to processing of individual data, and the basis for monitoring and retention of e-mail communications.

- **Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000** empowers the Secretary of State to make regulations, which allow businesses to intercept communications.

- **Contract law**. It is possible to make a legally binding contract via e-mail.

- **Copyright law**. The Copyright, Designs and Patents Act 1988 gives the same protection to digital and electronic publications as it does to other forms of publication.

- **Obscene Publications Act 1959**, Protection of Children Act 1988, Criminal Justice Act 1988. These Acts are concerned with material that might be criminal, cause harm to young persons or be otherwise unlawful.

- **Computer Misuse Act 1990**. This Act is mainly concerned with the problems of 'hacking' into computer systems.

- **Lawful Business Practice Regulations (LBP)** authorise employers to monitor or record communications without consent for a number of purposes.

5.8 Email Good Practice Guide

- **Message header, or subject -** Convey as much information as possible within the size limitation. This will help those who get many e-mails to decide which are most important, or identify those which are a priority.

- **Subject -** Avoid sending messages dealing with more than one subject. These are difficult to give a meaningful subject heading to, difficult for the recipient to forward on to others for action, and difficult to archive.

- **Replying** - When replying to a message sent to more than one person, do not routinely reply to all recipients of the original message. Consider who needs to read the reply, e.g. if the sender is organising a meeting and asking the recipient for availability dates, the recipient need only reply to the sender.

- **Email threads** - Include the previous message when making a reply. This is called a thread. Threads are a series of responses to an original message. It is best that a response to a message is continued by using "reply" accessed on the quick menu bar, rather than start an entirely new message for a response. Keep the thread information together. It is easier for the participants to follow the chain of information already exchanged. If the message gets too long the previous parts can be edited while still leaving the essence of the message.

- **Forwarding emails** - Consideration should be given when forwarding emails that it may contain information that the recipient should consult with the originator before passing to someone else.

- **Recipients -** Beware of sending messages to too many recipients at once. When sending messages for more than one person's use be sure to indicate people for whom there is some expectation of action or who have central interest; "cc" to indicate those who have peripheral interest and who are not expected to take action or respond unless they wish to do so.

- **Read Receipt -** When it is important to know that a recipient has opened a message, it is recommended that the sender invokes the 'read receipt' option.

- **Attachment Formats -** When attaching a file it will have a specific format. The sender should be aware of the possibility that a recipient may not have the software necessary to read the attachment. Format incompatibility can occur even between successive versions of the same software, e.g. different version of Microsoft Word.

- **E-mail Address Groups -** If messages are regularly sent to the same group of people, the addressing process can be speeded up by the creation of a personal group in the personal address book.

- **Absent** - It is possible for members of staff to set an 'out of office' message when s/he is going to be away for some time, e.g. on annual leave. Messages will not be lost, they will await the recipient's return, but the sender will know that the recipient is not there and can take alternative action if necessary.

- **Evidential Record** - Electronic conversations can produce an evidential record which is absent in a telephone conversation. Comments made by an employee during the course of an exchange of emails could be used in support, or in defence, of Mulberry UTC's legal position in the event of a dispute.

- **Legal records** - Computer-generated information can now be used in evidence in the courts. Conversations conducted over the email can result in legally binding contracts being put into place.

- **Distribution Lists** - Personal distribution lists should be kept up-to-date; individuals should be removed from lists that no longer apply to them.

- **Context** - Email in the right context; care should be taken to use email where appropriate. There may be occasions when a telephone call would be more appropriate especially on delicate matters. Beware of excessive use of capitals. It can be interpreted as SHOUTING so consider how the style of the email may be interpreted by its recipient. Consider the use of italics for emphasis, if required.

- **Large emails** - For larger emails, where possible send at the end of the day as they may cause queues to form and slow other people's email.

Disclaimer

Mulberry UTC makes no guarantees about the quality of the services provided and is not responsible for any claims, losses, damages, costs, or other obligations arising from use of the network or accounts. Any additional charges a user accrues due to the use of the school's network are to be borne by the user. The school also denies any responsibility for the accuracy or quality of the information obtained through user access. Any statement, accessible on the computer network or the Internet, is understood to be the author's individual point of view and not that of the UTC, the Mulberry Schools Trust, its affiliates, or employees.