E13
STAFF ICT ACCEPTABLE USAGE POLICY

Version 1.0

Policy Document
Last reviewed:
August 2023
Approved: Trust Board

Contents

ICT Acceptable Use Policy

1.0 Introduction

1.1 This policy sets out the acceptable use of Information and Communication Technologies within Esteem Multi-Academy Trust. Copies of this document are available on the HR/Payroll Portal.

1.2 The AUP will be reviewed every two years, updated as and when necessary. Members of staff will be informed of amendments.

1.3 If staff have any questions about the requirements of this AUP, then advice should be sought from their headteacher, school business manager or a member of the Esteem ICT or HR team (HR@esteemmat.co.uk).

2.0 Definition of Terms

2.1 The terms detailed below are used in this document and relate to the following:

a) Network User: any person that uses the school or Trust's network infrastructure.

b) Staff: for ease of reading, this policy will refer to all those listed below either staff or members of staff:

- Members of staff or workers employed by Esteem Multi-Academy Trust
- Members
- Trustees
- Governors
- Contractors
- Agency Staff
- Volunteers, including those on student/work experience placements working on behalf of the Trust.
- any adult who attends the school/Trust for education purposes.

c) Hacking: any attempt to bypass any of the school/Trust network's security or filtering systems.

d) School or Trust: any school or team within Esteem Multi-Academy Trust.

e) AUP – ICT Acceptable Use Policy.

f) Laptop/Device/iPad/Tablet/Computer: these terms are used interchangeable and refer to a connected electronic device.

3.0 Policies and Procedures

3.1 The ICT Acceptable Use Policy (AUP) is part of a suite of documentation which covers the safe and legal use of ICT within the Trust. These include (but are not limited to) Child Protection, Bullying, harassment and Victimisation Policy, Health and Safety, Professional Expectations Policy (Code of Conduct) and UK GDPR.

3.2 This AUP does not seek to address every possible circumstance, and simply because a particular action or unacceptable use may not be addressed within the AUP, this does not condone that action or misuse by omission.

3.3 Use of ICT is monitored, and cases of misuse by staff will be reported to the Headteacher. A log of any incidents may be retained in staff personnel files.

3.4 Where our filtering system detects attempts to access websites or materials considered to present a risk of harm it will automatically generate an alert that will be sent to the school's Safeguarding lead. (including, but limited to: intolerance, racism, terrorism, self-harm and/or relating to content of a sexual nature). These filtering reports may also be shared with external services to help us identify inappropriate or safeguarding issues.

4.0 Communication of concerns

4.1 Staff will be contacted directly where concerns exist regarding improper use of the Internet or ICT equipment. Improper use may result in staff members being temporarily or permanently restricted from systems and/or subject to disciplinary measures may be taken depending upon the nature of the abuse.

4.2 All misuse and ICT related issues will be dealt with under the E07 Esteem Disciplinary Policy.

5.0 Acceptable use guidelines for staff

5.1 All emails/communications/documents/etc. must be professionally worded which leaver the receiver in doubt as to the motives or integrity of a member of staff sending.

5.2 Any Trust ICT equipment or service utilised by a member of staff is provided for the primary purpose as a work tool, for work related duties only. It must not be used to conduct a personal business/enterprise for personal gain or to access/store any information/media/photos/files that could be seen to be inappropriate on the device.

5.3 Any electronic communication with other members of the school must be made using the internal school systems, taking into account that all communication/files must be of a professional nature.

5.4 Staff must keep their passwords secure and make sure their passwords are of significant strength. They must include a mixture of upper case, lower case and numbers to make it difficult for anyone to guess.

5.5 Passwords must not be given to any other members of staff or students at any time and care must be taken when typing passwords into a device/computer/laptop to make sure that no other person can identify the password or pin code.

5.6 Staff are responsible for the security and acceptable use of their laptop/device/network account.

5.7 Staff must ensure that their laptop and other computer equipment is stored securely when not in use. This means when equipment is taken offsite that they are not left in a motor vehicle or outbuildings such as shed or garages, away from the main occupied space, even if those spaces are used as a home office space.

5.8 Staff must not keep passwords with their laptop.

5.9 If a laptop is lost or stolen, a report must be made to the Police. Staff must provide the Police with a serial number which should be able to be located by the school business manager or ICT support.

5.10 ICT Support Team must be provided with the crime reference number for insurance purposes.

5.11 Data or files should not be saved onto the laptop internal hard drive and should be stored on the member of staffs OneDrive or school Sharepoint sites. The system will not remind the member of staff to do this, it is the responsibility of the member of staff to make sure this is carried out. Should a hard drive fail, you will not be able to recover lost data/files.

5.12 In relation to personal devices such as smartphones or tablets, any important work-related documents should be emailed to your own account or stored on the OneDrive to keep them safe should the device fail.

5.13 Staff are expected to maintain reasonable care with all portable equipment. This includes taking measures to ensure that the equipment is transported in a safe and secure manner. Any damage to Trust equipment must be reported immediately to the Headteacher.

5.14 Staff should be aware that all portable equipment, if stolen or damaged, is insured whilst in school or at home via the Trust's insurance, where forced entry can be proven. This insurance does not cover equipment which is stolen or damaged as the result of being left unattended, in a motor vehicle or other outbuildings.

5.15 All software should be installed by ICT Support and must have the relevant license made available to them before installation. Software without the correct license must not be installed and staff who attempt to install software themselves will be responsible for any damage caused to the item. This will also be investigated inline with the E07 Esteem Disciplinary Policy.

5.16 With mobile devices and Apps if you require a password to install the app this must be carried out by ICT Support (some devices may be unlocked to allow you to undertake this yourself).

5.17 Online learning systems (such as Kerboodle or Accelerated Reader) should be approved by the ICT Support team before being purchased or set up.

5.18 ICT Support maintains a software audit, containing a list of the software installed on each device. This audit will be made available to any official body who require it for the purposes of copyright enforcement. The use or copying of software without the licensor's permission is illegal and the terms and conditions of software licenses must always be adhered to.

5.19 The copying of music files, video and other copyright material if not legally purchased by the member of staff/students onto school computers may be illegal and removed if discovered. DVD's may only be played to an audience if it is within the terms of their license agreement or the school holds an additional license which allows this.

5.20 School mobile devices may be locked to not allow such content in which case no member of staff should circumvent this setting.

5.21 Whilst it is the user's responsibility to take reasonable care over the configuration of their computer hardware, it is possible for software to be installed on a machine without the full comprehension of the user. Users discovering software that has been installed in an unsolicited manner and which contravenes the licensing regulations above must contact the ICT Support team who will assist in resolving any issues.

5.22 The Trust has the right to seize/reclaim any laptop, computer, device, software or hardware, without explanation.

5.23 The ICT Support team have the ability to view all files on the network and devices but are prohibited from doing so without permission from the CEO, Deputy CEO, Head of HR, Head of Safeguarding, Headteacher, Chair of Governors or the Network Manager.

5.24 Staff must be aware of the UK GDPR legislation requirements and are prohibited from taking copies of any personal data about students or other members of staff during their employment or prior to and

including their leave date. Knowingly or recklessly obtaining, disclosing or procuring personal data without the consent of the Esteem data controller could be considered a criminal offence under the Theft Act 1968 and will be reported to the police and Information Commissioner's Office (ICO).

5.25 Contact with parents/carers should be made in line with the school agreed communication methods.

5.26 Any contact with pupils via electronic means must be for teaching and learning only and must only be carried out via the school's own systems (e.g., School email).

5.27 No use of personal email/social networking systems/mobile messaging etc. should ever be used to communicate with pupils for child protection and staff protection (e.g. allegations against a member of staff etc.).

5.28 Staff must report inappropriate messages, they receive, to the headteacher immediately.

5.29 Staff must report inappropriate website, images or video clips, if they discover one is accessible from the school network, to the headteacher.

6.0 UK General Data Protection Regulations (UK GDPR)

6.1 Data is stored in accordance with the regulations laid out by the UK GDPR. We will take every reasonable precaution to protect information. Appropriate physical, electronic and procedural safeguards are in place to ensure the security, integrity and privacy of all information kept in our MIS.

6.2 The need for confidentiality will be respected, and sharing of data will only occur with the express permission of staff in line with GDPR

6.3 All the staff must take their UK GDPR obligations very seriously and a main priority across each of our schools.

6.4 Staff must be committed to protecting and respecting the privacy of sensitive information relating to staff, pupils, parents/carers and those in a governance role.

6.5 Staff must ensure all data is processed in line with the requirements and protections set out in the UK General Data Protection Regulation, Esteem Confidentiality Policy and Esteem Retentions Policy.

7.0 Personally Owned Equipment

7.1 Staff are advised not to bring personally owned equipment (Laptops, Cameras, Tablets, Mobiles etc.) into school. However, if they do, they must be aware that they are not covered by the school's insurance and are brought into school at the owner's risk.

7.2 If personally owned equipment is used within school it should not be used to make recordings (video and/or sounds) of others if the other parties permission has not be sought prior to the recording.

7.3 Any personally owned equipment must be used in accordance to this acceptable use policy.

7.4 Such equipment may be placed onto the school's guest wireless network but will need to have adequate and automatically updating virus protection/security software.

8.0 Using Technologies Safely

8.1 All users of the school's systems (staff and students) must be aware that any electronic communication or document is open for public access/accountability and scrutiny via such legislation as the Freedom of Information Act and/or subject access request.

8.2 Internet

a) All Network Users must use their own network account to logon to the network. The School's auditing software automatically records the address of all websites accessed and this information can be retrieved by ICT Support.

b) All school/trust equipment and network use is filtered by the Trust or School's filtering system. This includes when used off school/trust sites, e.g. at home. Attempts to bypass the filtering system are strictly prohibited and may result in a user's Internet access being removed. All access matching safeguarding criteria is reported daily to a member of the safeguarding team.

c) ICT Support have access to unfiltered access for testing purposes and its use is governed by this AUP. Use of the unfiltered access must be sanctioned by the Trust ICT lead.

8.3 Email and Messaging

a) All Staff have an individual email account. All Network Users must use their school email account for all school related correspondence.

b) Staff should be aware that, where necessary, their email account may be monitored by the Network Manager/Head of ICT or Headteacher.

c) Staff should be aware that their school email account may be monitored, either randomly or where any suspicion has arisen. The random monitoring of the accounts will be done by the ICT Support team.

d) Where suspicion has arisen, the Network Manager/ICT Support team will be responsible for retrieving evidence from the server and/or equipment/systems.

8.4 Spam and Spoofing

a) The School/Trust uses the Microsoft Exchange Online Protection mail filtering service. This service reduces the amount of malicious, spam and spoofing emails but users should still be aware on how to recognise malicious, spam and spoofing or phishing emails and delete them immediately without opening them.

b) Malicious emails will either contain attachments or links containing malicious code that will attempt to steal data, lock access to the device or files and demand ransom (ransomware such as cryptolocker) or install other malicious software onto the network or devices.

c) Spam refers to unsolicited email or email that is sent without your permission, usually offering products or services. The subject of a spam message is usually designed to attract people to reading it.

d) Spoofing and Phishing refers to an email which claims to be from a bona fide company, such as a bank, requesting that you visit 'their' website and confirm your details or claim your prize/gift. These sites do not belong to the company they claim to be from and subsequently use your details to access your bank account. A genuine organisation would never ask you to confirm details in this manner or offer prizes/gifts you were not expecting.

8.5 Social Networking Sites and Chat Rooms

a) Staff should not access social networking sites or chat rooms on the school network – unless specifically instructed to as part of their job role.

b) Staff who wish to set up/access a social networking sites or visit a chat room (or similar) should do so in their own time, outside of the school's ICT system. Staff are advised not give away any personal information or put personal information for the public to view, such as their address, mobile telephone numbers, personal email address etc.

c) The school/Trust regularly monitor websites to discover any inappropriate material about the Trust, School, Staff etc and will take appropriate action where necessary.

8.7 Webcams

a) Where video conferencing/webcams are used within school, they should never be used to record people if they are unaware of the recording.

b) Staff should be aware that certain viruses and Trojans do exist which can activate a webcam without the owner's permission. Concerns of this nature should be reported immediately to the ICT Support team and Headteacher.

8.8 Peer-to-Peer (P2P) Networks

a) Staff forbidden from connecting to and/or downloading data from peer-to-peer networks.

b) Peer-to-Peer networks (such as Bit Torrenting, LimeWire, BearShare or Morpheus) often contain copyrighted content, viruses, spyware or other inappropriate materials and users should be aware that downloading torrents, and files from a Peer-to-Peer network may be illegal or compromise their computer.

9 Trust and School websites

9.1 Each school within the Trust and the Trust itself and some of its teams have their own websites. It is the responsibility of the School Business Manager/Team leader to ensure that all materials on their website do not infringe the intellectual property rights of others.

9.2 The School Business Manager/Team leader will take all reasonable steps to ensure that material created by the school and/or Trust is protected under copyright.

9.3 The School Business Manager/Team leader will ensure that the website is regularly checked for inappropriate content or material and that access to the website server is secured by a strong password to prevent unauthorised access.

9.4 The Trust/school cannot be held responsible for the content of external sites, even if they are linked to/from the Trust/school website.

10 Use of Staff and Student Photographs & Video (Images)

10.1 Students and staff will have their photographs taken both formally (by school photographers and for use on the school's information systems) and informally (for example trips/visits or around school during activities). If photos are to be used for media/website/publications/newsletters, then staff must ensure the correct level of permission has been obtained before they are published in the public domain.

10.2 Videos of students working may be taken by staff for internal feedback use or for assessment purposes to be sent to examination bodies, these recordings will not be made publicly available.

Appendix 1: Frequently Asked Questions

Introduction

The purpose of this frequently asked question sheet is to give generic examples of acceptable and safe use of the Trust/school's ICT systems in accordance with the above ICT acceptable usage policy. If at any point you are unsure as to what is acceptable or safe then please contact the ICT support team, Headteacher or School Business Manager who will provide advice or seek further guidance from an appropriate source.

Q: A student has emailed me from their own personal email address (eg. Hotmail, Googlemail). Can I respond to that email address?

A: No: You should reply to that student's school email account and not enter into communication using the external system. This must also be reported to the Headteacher.

Q: A student has asked me to be their 'friend' on Facebook (or other social network/online gaming system – Xbox etc). Can I accept them?

A: No: You should **not** make contact with students via any social networking site or messaging system (such as Whatsapp, Instagram, text messaging, etc). Any such contact should be reported to the Headteacher so follow up can occur with the student.

Q: Can anyone request my communication/files/messages? Do I need to keep my communication/files/ messages professional at all times?

A: Yes: All users of the school's systems (staff and students) must be aware that any electronic communication or document is open for public access/accountability and scrutiny via such legislation as the Freedom of Information Act. All emails/communication/documents/etc. must be professionally worded which leaver the receiver in doubt as to the motives or integrity of a member of staff sending.

Q: Students are doing a presentation from my laptop/device and need my password to log on/remove screensaver. Can I give it to them?

A: No: Your password has access to highly sensitive information and must be kept secure. Passwords must include a mix of uppercase letters, lowercase letters and at least one number to make sure they are secure. Care must be taken that when entering your password/passcode/pin that no other person is watching to try and obtain it for later use.

Q: I have been asked by an external contact/agency to provide them with a list of students in a year group. Can I send them this information?

A: No: Any personal information going to external parties must be agreed by the Headteacher or appropriate manager. Information is protected under the GDPR UK regulations and our fair processing notice (on school website). The Trust/school must have regards to this before transferring information to any external party.

Q: A parent has emailed me, and I need to respond. Can I email them back?

A: No: The response to the email should be made by phone, the agreed parent/communication portal/app or formal letter (letters must go via the admin support team before going home) and should be discussed with the Headteacher. Email is not acceptable as a response method where other parent/carer communication tools are available.

Q: Can I take my laptop/tablet/device home?

A: Yes: You can take devices home and connect to your home internet connection if desired. However, the laptop/tablet/device is for school use and must not be used to conduct a personal business/enterprise for personal gain (tax implications may exist). The laptop/tablet/device must be transported securely and safely. Where a device has been locked by ICT support no attempt should be made to circumvent the security in place. You must make sure that the device is not used to access any illegal or inappropriate content when connected to your own internet connection. If any such filters flag this or content is discovered this will be referred to the Headteacher who is likely to investigate in line with the Esteem Disciplinary Policy.

Q: Who is responsible for backing up my laptop/device?

A: You are. Please ensure all files are stored on the appropriate OneDrive or shared space. Laptop drives do crash or break. If you have important files on other devices (mobiles/tablets etc) please regularly email these documents to your school email account or upload to one of your school provided cloud storage areas.

Q: I am working with a student and they could benefit from using my device. Can they do this?

A: When working directly with students they can use your device but only under your direct supervision so you can ensure that they do not use the device to access anything they should not view such as your email or an area of the network that is only for staff.

Q: Can I install my own software (personally owned or purchased) on to my laptop/device?

A: You must seek permission from the ICT Support team. If you wish to have software installed that the school owns then please speak to your school business manager who will arrange for this to be actioned. For iPads/Tablets/Apps requests for installation can be made to ICT Support team who will evaluate the app against the cost and arrange installation if deemed acceptable.

Appendix 2: Laptop/Device Loan Agreement

Esteem MAT/Laptop Loan agreement.

School Name:
Device Make:
Model :
Serial Number :
Radio Lan Card MAC Address:
Date:

The laptop/device detailed above is loaned to for the duration of their employment at Esteem MAT subject to the following terms and the Trust/school's ICT policy.

The laptop/device must be returned to the school on ceasing to be employed at the school or if required during a planned absence.

1. The laptop/device is for the work-related use of the named member of staff to which it is issued.
2. Only software installed at the time of issue or software purchased by and licensed to Esteem MAT or its schools may be installed on the machine.
3. The laptop/device remains the property of Esteem MAT throughout the loan period. However the member of staff to which it is issued, will be required to take responsibility for its care and safe keeping.
4. The laptop/device is covered by Esteem MAT Insurance, when at home or school, providing it is not left unattended.
5. If left unattended the laptop/device should be in a locked room or secure area.
6. Due regard must be given to the security of the computer if using other forms of transport.
7. In order to ensure the school's compliance with GDPR UK regulations and to avoid breaches of confidentiality: under no circumstances should students be allowed to use the staff laptops/devices if not directly supervised by a member of staff.
8. Staff should also be cautious when using the computer away from school particularly with files which may contain personal student data.
9. The laptop/device will be recalled from time to time for maintenance/upgrade and monitoring.

I have read and agree to the terms and conditions in this agreement. I undertake to take due care of the computer and return it when requested.

Signed:
Date: