EBOR ACADEMY TRUST

Policy Number

12a

Acceptable Use Policy

Approved By:	Ebor Academy Trust Board of Trustees
Approval Date:	November 2021
Review Period:	Every 3 years
Review Date:	November 2024

`

Author:	*Tim Moat*
Date Created/updated:	*August 2021*
Version Number:	*2*

1. **Purpose**

   This document aims to provide clear guidelines for users of Information Communication Technology (ICT) at Ebor Academy Trust.

   The main purpose of this document is as follows:

   a) To safeguard and protect the children and users within schools/Trust

   b) To safely embrace new and emerging technologies if deemed to be of benefit to pedagogical practices within the Trust including but not limited to teaching and learning.

   c) To assist users working with children in the safe and responsible use of ICT and web-based services,

   d) To ensure that all staff are aware of their professional and legal obligations in regards to ICT responsibilities and expectations while working for the Trust.

Technological methods for keeping data secure are imperative, and the Trust believes that it is good practice to keep clear practical policies, backed up by written procedures.

This policy should be read in conjunction with the following related Trust policies:

- GDPR / Data Protection Policy
- CCTV Policy
- Records Management Policy
- E-Safety policy
- Trust IT Strategy

2. **Scope**

   This policy applies to all employees of the Trust however, where applicable, the individual sites may append additional guidelines to this policy based on a specific individual need or requirement.

   Therefore this would become a non-exhaustive policy and we recommend that you check with your establishment directly to obtain the complete policy set applicable to you.

3. **Roles and Responsibilities**

   Roles and responsibilities of individuals and groups within the Trust in relation to ICT security are defined in the IT Strategy, but every system user is responsible for:

   a) The security of their username and password which must not allow anybody else to access the ICT systems using their log-in details. To share these is a disciplinary matter.

b) Immediately reporting any suspicion or evidence that there has been a breach of security or that any password may no longer be secure.

c) Ensuring they have an up-to-date awareness of ICT security matters within the Trust

d) Ensuring all digital communications with any person via email or any other electronic messaging system are on a professional level and only carried out using official systems

e) Only monitoring learners' ICT activity in lessons, extracurricular and extended school activities when specifically authorised by their school

f) Remaining aware of security issues related to the use of mobile phones, cameras and hand-held devices and implement the appropriate policies accordingly

g) In lessons where internet use is pre-planned, guide learners to sites checked as suitable for their use.

h) Immediately report any unsuitable material that is found in internet searches to the Trust's IT Lead, Executive Head, or COO.

i) Filtering issues should be reported immediately to the Trust's IT Lead

j) Report any suspected misuse or problem relating to IT, including the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature, to their line manager or via the Whistleblowing Policy.

4. **Use of Trust issued IT equipment**

General principles

a) A school or Trust issued mobile telephone, laptop, tablet computer or similar electronic device, must only be used in accordance with this policy and any other instructions given by the Trust or school, and shall not use such a device for any unauthorised purpose.

b) Do not access or attempt to access school or Trust ICT systems using another person's account

c) Do not attempt to gain access to restricted areas of the network, or to any password protected information, unless specifically authorised by the Trust's IT Lead

d) Do not breach any Trust policies with regards use of IT

e) Do not establish Internet or other external communications connections that could enable a third party to access our computer systems

f) Immediately report any damage or faults involving equipment or software, however caused, to the Trust's IT supplier

g) Ensure that any electronic device used is properly “logged-off” at the end of any session and initiate a password-protected screensaver when leaving their computer unattended to prevent anyone else accessing the network using their log-in identity

h) Ensure the device is stored safely and securely, especially overnight.

5. **Use of portable devices**

a) When data is stored on any portable computer system, USB stick or any other removable media: the device must be encrypted and password protected; the device must offer approved virus and malware checking software; the data must be securely deleted from the device once it has been transferred or its use is complete; the device must be kept in a locked filing cabinet, drawer or safe when not in use

b) Any System User who uses a tablet computer or other hand-held device away from Trust or school premises must take appropriate additional precautions to safeguard the security of such equipment. Such precautions include but are not limited to keeping the device either with the System User or in a secure location at all times.

6. **Data security**

a) Users must at all times take care to ensure the safekeeping of school and Trust ICT systems to minimise the risk of loss or misuse.

b) Users must store school and Trust information on the central ICT network, the retention of Trust information on personal devices is prohibited.

c) Documents, tablet computers and other devices containing Trust or school information should never be left unattended. In the event that any such device is lost or stolen, or a System User believes that it may have been accessed by an unauthorised person or otherwise compromised, they must report it immediately.

d) Emails should only be retained in System Users’ inboxes or elsewhere on the network for as long as they are needed for the purpose for which they were sent or received. Any email containing personal details **must** always be deleted, once used for the purpose sent. All retention periods are specified in the Trust’s Document Retention Policy.

e) Users will be deregistered from systems on the day they leave and will not be allowed access to data after that point.

7. **Banned use of Trust ICT systems**

System Users ***shall not:***

Visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments which are offensive, obscene, demeaning, indecent, disruptive or discriminatory. This includes but is not limited to material that contains or relates to:

a) Child sexual abuse images

b) Promotion or conduct of illegal acts, e.g. under the child protection,

c) Computer misuse and fraud legislation

d) Adult material that potentially breaches the Obscene Publications Act in the UK

e) Pornography

f) Promotion of any kind of discrimination

g) Promotion of racial or religious hatred

h) Promotion of threatening behaviour, including promotion of physical violence or mental harm.

Further; System Users must not use any Trust ICT systems for:

a) Running a private business

b) Excessive or inappropriate personal use including but not limited to online gaming or video broadcasting, online gambling, accessing social networking sites

c) Accessing or using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school or the Trust;

d) Upload, download or transmission of files, commercial software or any copyrighted materials belonging to third parties without the necessary licensing permissions;

e) Creating or propagating computer viruses or other harmful files;

f) Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet;

g) Corrupting or destroying the data of any other person or causing deliberate damage to hardware or software;

h) Downloading materials from unknown source

i) Post personal information on any school or Trust website or social media pages

j) Posting defamatory comments that could bring the Trust or any of its employees into disrepute.

k) Reveal or publicise confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)

8. **Communications:**

a) Any digital communication between System Users and learners or parents (e.g. via email or any other electronic messaging system) must be professional in tone and content. These communications may only take place on official Trust systems.

b) The Trust's email service may be regarded as safe and secure. System Users should therefore use only the Trust's email service to communicate (e.g. by remote access).

9. **Software**

Employees must not install or download any hardware or software to a Trust device; this must be done via the IT supplier.

10. **Use of Personal IT**

a. Laptops

I. Due to safety reasons, staff may only use their own devices if they have been PAT tested. This also conforms with Trust insurance requirements

II. Trust insurance will not cover damage to personal devices on site, but it will cover harm to others by way of an accident involving the equipment.

III. Employees must not use their personal laptops for processing personal or special category data. Such information should only be processed on a secure network using school or Trust equipment. Lesson planning and work of anonymised groups or any work of a non-personal nature may be performed on a staff member's own device. If the System User has any queries regarding this then they must seek the advice of the Trust's Director of Governance and Risk

IV. Members of staff are not permitted to use their own personal phones, tablets, laptops, personal computers or similar devices for contacting children, young people and their families within or outside of the setting in a professional capacity. Any pre-existing relationships which could compromise this will be discussed with managers/Principals.

V. Laptops must not be used to capture pictures or recordings of children.

VI. Staff will not add parents of the school that they work in as friends on any personal social media accounts. Any staff who have pre-existing connections with parents will make line managers aware of this.

b. Staff use of personal mobile phones

Members of staff will ensure that any use of personal phones and devices will always take place in accordance with the law as well as relevant Trust policy and procedures, particularly Data Protection and Safeguarding and Child Protection.

I. Early Years staff must not use personal phones and devices in classrooms or settings at any time.

II. Staff personal mobile phones and devices must be switched off/switched to 'silent'; and not be used during teaching periods unless permission has been given by a member of the Leadership Team in emergency circumstances.

III. Staff will ensure that any content bought on site via mobile phones and personal devices are compatible with their professional role and expectation**s.**

IV. Staff will not use any personal devices directly with children and will only use work-provided equipment during lessons/educational activities.

c. Staff use of social media sites outside of work

I. Although these networks are used by staff in their own time, staff must not discuss issues relating to children or other staff via these networks.

II. Staff are encouraged to review their privacy settings to make sure that their profiles and photographs are not viewable by the general public.

III. It is never acceptable to accept a friendship request from a child from the school as in almost all cases children of school age using such networks will be breaching the terms and conditions of use of those networks. It is also extremely inadvisable to accept as friends ex-pupils who are still minors.

11. **Digital and Video Images**

a) System Users must only take digital/video images using a school/Trust-issued camera or school/Trust-issued portable device. Personal equipment of System Users must not be used for such purposes.

b) System Users may take digital/video images to support educational aims, but must follow the rules below concerning the sharing, distribution and publication of those images.

c) When taking digital/video images, learners must be appropriately dressed and not be participating in activities that might bring the individuals, the school or the Trust into disrepute.

d) Learners must not take, use, share, publish or distribute images of others without their permission.

e) Written consent from the relevant learner's parent/carer must be obtained before any photograph or video of any learner is published internally or externally (e.g. on display boards and screens, or on the school's or the Trust's website, Twitter and Facebook pages).

f) Learners' full names must not be used anywhere on any external publication (e.g. website or social media).

12. **Monitoring of use**

a) System Users should note that the computer network and email system is the Trust's property.

b) The Trust expressly reserves the right to monitor the use at work of email and the internet in the ordinary course of business, and at the Trust's discretion. "Deleted" material remains on the system and may still be monitored by the Trust.

c) The Trust may delete messages or prevent messages being sent from the email system at its discretion, and disclose details about System Users' use of email and the Internet as required to comply with legal and contractual obligations.

d) Access to emails and data may be required in rare cases, such as in cases of unexpected absence or departure. The application process is laid out in the IT Strategy.

13. **Responding to Incidents of Misuse or breach of policy**

Each System User has a duty to be a responsible user of ICT and to follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

Listed below are the responses that will be made to any apparent or actual incidents of misuse:

a) Any System User found to be in breach of this policy may be subject to disciplinary proceedings which in serious cases, or in cases of repeated breach, may result in dismissal. Any System User who is in any doubt about the terms of this policy or has any questions regarding this policy should contact Ebor's IT Lead for further guidance.

b) If any apparent or actual misuse appears to involve illegal activity including child sexual abuse images, adult material which potentially breaches the Obscene Publications Act or criminally racist material then the police and LADDO will be contacted.

14. **Additional Information**

This policy does not form part of any employee's contract of employment and it may be amended by the Trust at any time. Any changes will be notified in writing.

This policy will be reviewed every two years to ensure it is achieving its stated objectives

AGREEMENT

I recognise the value of the Ebor Academy Trust's IT systems for enhancing learning, and organisational efficiency and will ensure that 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 online safety in my work with young people.

I understand that I have a duty to report any breaches of this policy to my line manager as soon as practicable.

I agree that:

1. Ebor Academy Trust may monitor my use of the ICT systems, email and other digital communications
2. The rules set out in this agreement also apply to use of the Trust's systems (e.g. notebooks, email, etc.) out of school
3. ICT systems are intended for educational use, or to support the efficient running of the Trust
4. I will not disclose my password to anyone else, nor will I try to use any other person's username and password
5. I understand that I should not write down or store a password where it is possible that someone may steal it
6. I will always get permission before installing, attempting to install or storing programs of any type on the computers
7. Damaging, disabling, or otherwise harming the operation of computers, or intentionally wasting resources puts work at risk, and will cut short time with the ICT equipment. Therefore, I will not attempt to repair, alter or modify the hardware or firmware of any system, unless I have obtained permission from the CEO / COO
8. Use of school ICT equipment should be used for work purposes only
9. Personal activities such as buying, selling goods, checking personal email, use of chat rooms or social media may be investigated.
10. I will not connect a mobile device or piece of storage equipment (e.g. laptops, tablet PCs, PDAs etc.) to the network without permission.
11. If I have access to a mobile phone or device owned by the Trust, I am aware and will adhere to the rules of how these can be used, on the site/sites that I work at.
12. I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
13. I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of to the appropriate person.

14. I will be professional in my communications and actions when using school ICT systems:

15. 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.

16. I will only use my work email address when communicating on behalf of the Trust or any of its members.

17. I will ensure that when I take and/or publish images of others I will do so with permission and in accordance with the school's policy on the use of digital / video images.

18. I will not use my personal equipment to record images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.

19. I will carefully consider any image or comment that I upload, share or repost on social media, to ensure that the safety and reputation of the Trust are maintained

20. I will endeavour to look after and protect ICT equipment in the appropriate manner.

21. I will take reasonable precautions to protect work devices from accidental damage.

22. I will only communicate with students and parents/carers using official school systems as agreed by my line manager. Any such communication will be professional in tone and manner

23. I will not engage in any online activity using school systems or devices that may compromise my professional responsibilities.

24. When I use my personal handheld or external devices as outlined in the policy in school, I will follow the rules set out in this agreement, in the same way as if I as using equipment belonging to the Trust or one of its members.

25. 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

26. 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.

27. 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.

28. I will not try (unless I have permission) to make large downloads (in excess of 1GB) or uploads that might take up Internet capacity and prevent other users from being able to carry out their work.

29. 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.

30. I will only share personal information about myself or authorised others securely. Where personal data is transferred outside the secure school network, it will be encrypted.

31. I understand the data protection policy requires that any staff or student 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.

32. I will immediately report any damage or faults involving equipment or software, however this may have happened.

33. 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), outside what is allowed by UK Law.

34. I understand that all Internet activity is closely monitored and any misuse will be reported to senior leadership team for investigation and action will be taken if this privilege is misused.

35. When using social media site, I will not: - Reveal confidential information about our pupils, staff, or the Trust, engage in activities on the internet which might bring the Trust into disrepute - Use it in any way to attack or abuse stakeholders - Post defamatory, derogatory or offensive comments on the Internet about colleagues, pupils or the Trust.

36. I understand that I am responsible for my actions in and out of work and that this Acceptable Use Policy applies not only to my work and use of Trust ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school, as well as my use of personal equipment in school or in situations related to my employment by the school.

37. I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action which could include, but is not limited to, a warning, a suspension, referral to the Trustees and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the Trust's ICT systems and my own devices within these guidelines.

School/Site: ----------

Name: ----------

Date: ----------

Job Title: ----------

YOU SHOULD RETAIN A COPY OF THIS AGREEMENT FOR YOUR RECORDS AND REFERENCE
A COPY WILL BE HELD ON YOUR EMPLOYEE RECORD FOR THE DURATION OF YOUR EMPLOYMENT