THE
EDUCATION
ALLIANCE

ICT Acceptable Use Policy

Version 3.4

Important: This document can only be considered valid when viewed on the VLE. If this document has been printed or saved to another location, you must check that the version number on your copy matches that of the document online. **Name and Title of Author:**	Lisa Pipes, Director of HR and Governance
Name of Responsible Committee/Individual:	Trust Board
Implementation Date:	February 2020
Review Date:	February 2022
Target Audience:	All stakeholders
Related Documents:	Expectations and Code of Conduct Data Protection Policy Whistleblowing Policy Dignity at Work Policy Use of Equipment and Assets Policy Child Protection and Safeguarding Policies Disciplinary Policy and Procedure

Contents

Appendices

POLICY STATEMENT

We are here to make great schools and happier, stronger communities so that people have better lives. We do this by:

- Always doing what is right
- Trusting in each other and standing shoulder to shoulder
- Doing what we know makes the difference

Doing what is right means always acting with integrity, in the interests of others and being honest, open and transparent.

The purpose of this policy is to ensure that employees, workers and other people accessing Trust Information Communication Technology (ICT) understand the ways in which the ICT equipment and Wi-Fi is to be used. Our aim is to provide a service within schools to promote educational excellence in ICT, innovation, communication and educating users about online behaviour, including interacting with other individuals on social networking websites and in chat rooms, and cyber bullying awareness. The policy aims to ensure that ICT facilities and the Internet are used effectively for their intended purpose, without infringing legal requirements or creating unnecessary risk. Where reference is made to Trust ICT, this also includes any school specific facilities, equipment and networks. Any reference to Trust includes its schools.

Employees are provided with free access to a wide range of ICT provision to enable and assist their work and support their educational development. By using the Trust's provision, or using personal devices on-site, which may require access to the Trust’s Wi-Fi, all users are agreeing to adhere to this policy. When logging on to any computer in the Trust, users are presented with an informational message that alerts them to the fact that they are bound by the terms in this, and all related policies. All users must click 'OK' to show that they agree to the policies before they can continue to use the systems. This action is considered as further agreement to the terms of this policy.

Users are responsible and personally accountable for their use and activity on the Trust's ICT systems and Wi-Fi. Any use that contravenes this policy may result in the Trust Disciplinary Policy and Procedure being invoked. In addition, ICT usage privileges may be withdrawn or reduced.

1. SCOPE

This policy applies to all employees, workers and others accessing ICT at The Education Alliance and they will be termed as ‘users’ within this policy. This policy details the Trust’s expectations of all users of the Trust’s electronic communication, including, but not limited to telephone, social media platforms, email, internet and ICT systems.

2. ROLES AND RESPONSIBILITIES

The **Trust Board** is responsible for monitoring the effectiveness of this policy, ensuring that a consistent approach to ICT is applied across the Trust.

The **CEO** is responsible for ensuring that staff and managers are aware of and adhere to this policy and procedure and that breaches are managed swiftly and effectively.

The **IT Department** in each school is responsible for ensuring that all employees understand their responsibilities when using ICT at work and that systems are used and managed effectively. The IT Department will limit access to websites and may be directed to monitor usage and report any breaches to the Head of School, Executive Principal or CEO.

Managers must ensure they report any breaches of this policy immediately to the IT Department or Head of School.

All **users** must ensure they understand and adhere to the Trust's expectations regarding electronic usage and communications, seeking further clarification and advice where appropriate. If they require access to a website, which is blocked, they should raise the issue with their line manager and the IT Department.

3. EQUALITY AND DIVERSITY

The Education Alliance is committed to:

- Promoting equality and diversity in its policies, procedures and guidelines
- Ensuring staff are protected from unlawful direct or indirect discrimination resulting from a protected characteristic (e.g. age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex or sexual orientation)

4. KEY PRINCIPLES

This policy details the minimum expectations of the Trust when users are accessing Trust ICT systems and Wi-Fi. Failure to comply with these requirements may be viewed as a breach of this policy and could be viewed as a disciplinary matter, with serious breaches potentially leading to dismissal.

- Passwords and login details must remain confidential
- Users must not intentionally install software unless specifically authorised to do so
- Users must not intentionally introduce viruses or other malicious software

The Trust's e-communications systems must not be used to:

- Store, send or distribute messages or material which may be perceived by the recipient or the Trust as:
    - ➢ Aggressive, threatening, abusive or obscene
    - ➢ Sexually suggestive
    - ➢ Defamatory
    - ➢ Sexually explicit
    - ➢ Discriminatory comments, remarks or jokes
    - ➢ Offensive
- Act in a way that contravenes the Trust's Expectations and Code of Conduct, other Trust or school policies, legislative, statutory or professional requirements
- Bring the Trust/School into disrepute
- Disclose sensitive information or personal data to unapproved people or organisations
- Breach the Trust's Data Protection Policy, General Data Protection Regulations or the Data Protection Act 2018
- Intentionally access or download material containing sexual, discriminatory, offensive or illegal material
- Participate in online gambling, including lotteries
- Participate in online auctions unless authorised to do so for work-related matters
- Originate or participate in email chain letters or similar types of communication
- Harass or bully another person
- Create material with the intent to defraud

If a user accidentally accesses inappropriate material on the internet or by email, they must immediately disconnect and inform their manager or the IT Department.

Users must not bring into school any material that would be considered inappropriate. This includes files stored on memory sticks, CD, DVD or any other electronic storage medium, or accessing information via the Trust's Wi-Fi, which would be viewed inappropriate. Under no circumstances should any users of the Trust or school's ICT systems download, upload or bring into school material that is unsuitable for children or schools. This includes any material of a violent, racist or inappropriate sexual nature. The transmission, display, storage or promotion of any such material is a violation of the Computer Misuse Act 1990, and possession of certain types of material can lead to police prosecution. If in any doubt, staff should check with their line manager of the IT Department. Staff are also encouraged to refer to the film classification system as a guide.

Users must not use the Trust ICT systems or Wi-Fi for the creation, transmission or access of pornographic, illegal or gambling content.

Occasional appropriate and reasonable personal use of ICT equipment and or Wi-Fi on-site is permitted provided such use of the Trust systems:

- Is restricted to the user's own time
- Doesn't interfere with the performance of duties
- Doesn't adversely impact on the performance of the Trust's ICT systems or the network
- Doesn't contravene the requirements of the Trust's Expectations and Code of Conduct, or other Trust or school policies
- Doesn't include material of a pornographic, illegal, or gambling nature

Users must always be mindful that they are responsible and personally accountable for their use of Trust ICT systems and networks. All internet-based activity on personal devices is monitored and logged whilst using the Wi-Fi. Misuse of Trust ICT systems and networks belonging to, or associated with the Trust may breach the Expectations and Code of Conduct, other policies and/or procedures and/or the law. Users can be held personally liable and such breaches may lead to civil, criminal or disciplinary action including dismissal.

Users are responsible for all files that are stored in their storage area and any visits to websites by their user account. Users must not breach the copyright of any materials whilst using the Trust's ICT systems. This includes, but is not exclusive to:

- Copying, or attempting to copy, any of the school's software
- Storing any files in their personal storage area which require copyright permission, and where that permission is not held.

Any breach of copyright whilst using the Trust's ICT systems is the individual user's responsibility and the Trust cannot accept any liability or litigation for such a breach.

Users must ensure that:

- They keep personal data safe, taking steps to minimise the risk of loss or misuse of data
- Personally identifiable and sensitive, confidential data is protected with the use of passwords, locking of computers, logging off shared devices, use of encryptions where appropriate and increasing the use of remote access rather than transporting or transferring information
- Personally identifiable, sensitive and confidential data must not be stored on any form of removable media (e.g. memory sticks, external hard-drives, surfaces or lap tops, and CDs or DVDs) and it must not be stored on users' personal devices (e.g. home PCs, mobile 'phones)

- When using mobile devices (e.g. surfaces and lap tops) users encrypt/password protect documents; password protect the device; ensure the device has appropriate virus and malware checking software
- Data is only retained, destroyed and deleted safely in line with the Trust's Data Protection Policy and associated procedures and guidelines

Users are encouraged to use remote access, onedrive, google drive or Foldr where possible rather than memory sticks.

Memory sticks are an extremely insecure method of transferring data, they should be encrypted (password protected) to avoid any loss of data. Users must not download copy or attempt to install any software onto Trust computers/devices without checking first with their line manager and the IT Department. Any attempt by a user to compromise the security or functionality of the Trust networks and its ICT systems, either internally or externally, will be considered as "hacking". It should be noted that "hacking" is illegal under the Computer Misuse Act 1990 and is prosecutable under law. Users must not deliberately attempt to gain unauthorised access to networked facilities or services, including any attempt to probe, scan or test the vulnerability of the system or network. All machines connected to the Trust's ICT networks, must have appropriate, fully functioning and up to date antivirus software protection. If unsure, staff should seek advice from the IT Department.

Users must not discuss or post content that reflects the Trust or its employees in an inappropriate or defamatory manner through any electronic communication methods. This includes posting to social networking sites.

Users must not carry out any of the following deliberate activities:

- corrupting or destroying other users' data
- violating the privacy of other users
- disrupting the work of others
- denying service to other users (for example, by deliberate or reckless overloading the network)
- continuing to use an item of networking software or hardware after the Trust has requested that use cease because it is causing disruption to the correct functioning of the school's ICT systems and/or networks
- other misuse of the Trust's ICT and networked resources, such as the introduction of viruses or other harmful software to the Trust's ICT systems
- unauthorised monitoring of data or traffic on the Trust's ICT network or systems without the express authorisation of the owner of the network or systems

This policy still applies when users access any of the Trust's systems off-site.

The Trust wishes to encourage all users to use the internet, however it is provided for work purposes and any use of the internet for personal reasons must be carried out in the user's free time. The Trust cannot be held responsible for any failed personal financial transaction that may happen whilst using the Trust's ICT systems.

Any attempt to circumvent the Trust's firewall and internet filtering systems will be treated as a breach of this policy. This includes the use of proxy servers and websites to bypass the internet filtering systems. Such activity will be subject to the Trust's Disciplinary Procedure in addition to any disciplinary outcome or sanction; it could also result in the removal of access to the Trust's ICT systems or internet access.

There is a wealth of information on the internet; however, due the open nature of the internet, some material is either illegal or unacceptable. Any user who thinks inappropriate or illegal material is being accessed must report it to their line manager or the IT Department.

Whether users are using on-site Trust equipment, Trust equipment off-site or their own device via the Trust network, Users should:

- limit personal use of the internet to own time
- take advice from line managers before downloading large files or sending large amounts of data via a web-link – to avoid adversely impacting on the performance of the systems these transactions can be scheduled for off-peak times
- if users accidentally access inappropriate material including unexpected 'pop-ups' they must disconnect immediately and inform their line manager and/or the IT Department

Users must be mindful that if they use Trust equipment off-site, they need to minimise the risk of inappropriate information presenting on their Trust equipment whilst at work. For example, the acceptance of cookies can result in pop-ups, which may contain material, which is inappropriate for school environments.

Users must not:

- access or download material which is pornographic, illegal or of a gambling nature
- use the internet for personal use during working time, even if minimised on the screen
- use systems to participate in on-line gambling or on-line auctions
- download music or video files unless for Trust or school purposes
- use 'peer to peer' or other file sharing services except where authorised to do so

5. EMAIL AND ELECTRONIC COMMUNICATION ACCEPTABLE USE

When using Trust equipment, networks, email and electronic communication, the Trust expects all users act responsibly and strictly according to the following conditions.

- Email facilities are provided as a method of enhancing communication of work and school related issues. All users are responsible for the content of the messages that they send.
- Users are reminded that electronic communication can be monitored and random checks may be made.
- Email is the equivalent of a written document and can be used as an evidential record. With this in mind, care and consideration should always be taken before sending an email (e.g. freedom of information requests and subject access requests).
- Where there is a concern that a user has misused the email system, action may be taken in line with the Trust's Disciplinary Procedure.
- All electronic communication between staff and students must be carried out through the Trust's ICT systems.

Staff are advised not to communicate with students via social network sites, texts or telephone calls, although there may be occasions where it is appropriate and necessary (e.g. where staff and students are members of external groups or family and friend networks). If staff are unsure, they should seek advice from their line manager in the first instance. Staff must not share personal contact details to students (mobile telephone numbers, non-work email addresses, social networking sites etc.) unless there is a justifiable reason (e.g. family or friend networks or external groups) and any unintended breach must be reported to the IT Department and the user's line manager immediately.

Users who receive emails regarding viruses or security threats must delete the email and report to the IT Department. Users can minimise the risk of inadvertently introducing viruses by permanently deleting without opening emails that look suspicious. Staff are encouraged to contact the IT Department for advice and concerns that a virus may have entered a Trust system should be reported to the IT Department immediately.

Users should ensure:

- personal email and texts should only take place in their own time
- ensure that their messages are relevant and appropriate to targeted recipients (e.g. not using ‘blanket’ or ’all-user’ emails)
- try to answer emails quickly, politely and professionally
- beware of ‘email rage’. Email is quick and easy to use and can encourage ill-considered and even offensive messages
- include a subject heading in every email so that the person receiving it knows what it is about
- inform management immediately if the user receives or sees any offensive or sexually explicit material, spam or phishing communications on the intranet or in email messages at work
- they do not allow email and electronic communication to replace face to face communication

Users must not:

- use mobile phones, in classrooms in front of students, unless they have sought permission from their line manager to do so as part of their lesson
- use a password in a way that can be seen by students
- use email to circulate material which is illegal, pornographic or of a gambling nature
- use email as a substitute for good verbal communication
- expect to receive a response to emails outside of normal working hours

If staff are in doubt, they should seek advice from their line manager or the IT Department.

6. SOCIAL MEDIA AND ACCEPTABLE USE

Social networking websites provide an opportunity for people to communicate ‘en masse’ and share ideas regardless of geographical distance. Sites such as Facebook, Twitter and Linkedin can serve as a learning tool where training videos and other materials are made easily accessible to students in a user-friendly and engaging way. They can also be a useful tool for schools to communicate key messages to their community and the wider public. However, the open nature of the internet means that social networking sites can leave people vulnerable if they fail to observe a few simple precautions. The below guidelines are intended not as a set of instructions, but general advice on how to avoid compromising your professional position.

Privacy

Staff should ensure their Facebook accounts do not compromise their professional position and they should ensure that their privacy settings are set correctly. Staff should also be aware that settings can change and they should regularly review their list of friends.

Staff must not, under any circumstances, accept friend requests from a person they believe to be either a parent or a student at a school within the Trust. The exception to this is if an employee’s own child(ren) attend a Trust school or if close friends have children at a Trust school or are employed by the Trust. In these circumstances, it is accepted that communication can take place and that images of their own children and their friends when at parties or such similar personal events may be posted. Care should be taken to ensure the suitability of the images and to use appropriate security settings. Images must not be posted in relation to the school. Staff should seek advice from their line manager in such circumstances.

Conduct on social networking sites

- Users must not make disparaging remarks about their employer/colleagues.
- Users must act in accordance with this policy and any specific guidance on the use of social networking sites.
- Users are encouraged to think about any photos they may appear in and on Facebook; they may wish to 'untag' themselves from a photo.
- If a user finds inappropriate references to themselves and/or images of them posted by a 'friend' online, they are encouraged to contact them and the site to have the material removed.
- Staff are reminded that parents and students may access their profile and could, if they find the information and/or images it contains offensive, complain to the Trust.

If users have any concerns about information on their social networking sites or if they are the victim of cyber-bullying, they should contact their line manager.

When using social media either at work or in their own personal time, users must not:

- make defamatory statements about the Trust, its schools or its employees
- post messages or undertake activities that are unlawful.
- post content copied from elsewhere, for which the user does not own the copyright without proper permission and attribution

Under no circumstances should a member of staff have students as friends on social networking sites without seeking prior permission from their line manager. This poses a large risk to both students and staff, as the Trust has no control over the content that is made available through these sites.

7. MONITORING

Authorised officers of the Trust and its school's ICT providers may at any time monitor the use of Trust ICT systems and networks. The use of all Trust ICT systems and networks, particularly email and the internet, is subject to recording in order to detect and deal with abuse of the systems and fault detection. The Trust will not, without reasonable cause, examine any private material that is discovered.

Personal data should not be stored on the network and users should not expect 'privacy' in relation to accessing websites, personal email correspondence, personal documents stored on Trust ICT equipment or networks or messages sent via the internet, as these, in principle, are subject to the same checking procedures applied to business related access and email correspondence.

8. PASSWORDS

The Trust is responsible for ensuring data and the network is as safe and secure as possible. A weak password may result in the compromise or loss of data. As such, all users are responsible for taking the appropriate steps, as outlined below, to create and secure their passwords.

The aim of passwords is to protect user's data, children's welfare where access to confidential and sensitive data is allowed and to minimise the risk of unauthorised access to the Trust and school networks. The Trust enforces password changes each term, and advises that:

- Passwords will be a minimum of six characters
- Passwords should not contain the user's account name or parts of the user's full name that exceed two consecutive characters. They should contain characters from three of the following four categories:
    - Uppercase characters (A through Z)

- Lowercase characters (a through z)
- Base 10 digits (0 through 9)
- Non-alphabetic characters (for example, !, $, #, %)

9. MONITORING COMPLIANCE WITH AND EFFECTIVENESS OF THE POLICY

Effectiveness and compliance of this policy will be regularly monitored by the Trust IT Manager.

10. REVIEW

This Policy and Procedure will be reviewed within two years of the date of implementation with recognised trade unions via the Trust’s JCC.

Appendix 1

Advice Relating to Facebook Use

As a minimum, the Trust recommends the following when staff use Facebook:

Privacy Setting Recommended security level
Send the user messages - friends only
See the user’s friend list - friends only
See the user’s education and work - friends only
See the user’s current city and hometown - friends only
See the user’s likes, activities and other connections - friends only
View the user’s status, photos, and posts - friends only
Family and relationships - friends only
Photos and videos - friends only
Religious and political views - friends only
Birthday - friends only
Permission to comment on your posts - friends only
Places you check in to - friends only
Contact information - friends only

Users must always make sure they log out of Facebook after using it, particularly when using a machine that is shared with other colleagues/students. The user’s account can be hijacked by others if the user remains logged in – even if they quit the browser and/or switch the machine off. Similarly, Facebook’s instant chat facility means conversations can be viewed later on. Users must ensure they clear their chat history on Facebook (click “Clear Chat history” in the chat window).