ACCEPTABLE USE OF IT POLICY

(Potteries Network)

Potteries Educational Trust

Policy Family	Information Governance
Reference	SFC-21

Responsible Manager	IT Services Manager

Approval Date	May 2023
Issue Number	3
Review Date	May 2024

Aim

The purpose of this policy is to ensure that all individual academy and Trust stakeholders are aware of the Trust's requirements concerning the acceptable use of ICT facilities and understand and accept the Trust and academy's right to monitor communications using such facilities. It follows that to enable the Trust to provide protection against the risks and liabilities inherent in the use of communication systems such as email and the internet it is necessary for all network users to sign this document signifying their agreement to be bound by the regulations found within. This policy replaces previous versions of the Acceptable Use Policy and the Network user's form.

Scope

This policy concerns all students, employees (new and existing), consultants, contractors, governors/trustees, and volunteers, for the purposes of the policy known as network users.

Policy

1. General Points:

1.1. The Trust has the right to monitor all aspects of its telephone and computer systems that are made available and to monitor, intercept and/or record any communications made by network users, including telephones, e-mail, local-area-network, or internet communications. To ensure compliance with this policy or for any other purpose authorised under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 staff are hereby required to expressly consent to the Trust doing so. This consent is given by agreeing and signing the AUP delivered by Impero to every user account on the Potteries network, this is recorded and reset every Term to remind users of their rights and responsibilities on the Potteries network. The AUP may also be printed and signed, to be kept in your personnel file.

1.2. Computers and e-mail accounts are the property of the Trust and are designed to assist in the performance of Trust and/or academy work. Therefore, there should, have no expectation of privacy in any e-mail sent or received whether it is of a business or personal nature.

1.3. It is inappropriate use of e-mail and the Internet for network users to access, download, or transmit any material, which might reasonably be considered obscene, abusive, sexist, racist, or defamatory. You should be aware that such material might also be contained in “jokes” sent by e-mail. Such misuse of electronic systems will be misconduct. The Trust reserves the right to use the content of any network user e-mail, internet ‘history’ or network usage in any disciplinary process.

1.4. Users are required to escalate identifies faults to any network asset to the local academy IT Support.

2. Examples of Un-acceptable use:

2.1. Corrupting or destroying other user’s data
2.2. Violating the privacy of others
2.3. Disrupting the work of other users
2.4. Using the network in a way that denies service to others, e.g., deliberate overloading of printing facilities, deliberate overloading of access links (Internet link), excessive downloading without prior authorisation from IT.
2.5. Deliberate or thoughtless introduction of a virus into the network environment
2.6. Installation of unauthorised software on machines on the Potteries network.
2.7. Defamatory remarks in e-mails
2.8. Downloading, storing, or transmitting any material, which might be considered obscene, abusive, sexist, racist, or defamatory.

3. Network Service Guidance, E-Mail, and the Internet

3.1. E-mails should be drafted with care. Due to the informal nature of e-mail, it is easy to forget that it is a permanent form of written communication, and that material can be recovered even when it is deleted from a computer.

3.2. The Trust email system is for Trust and academy business use only – the sale of personal goods, advertisement and/or anything else that does not relate directly to academy business is strictly prohibited. Misuse in this way may be treated as misconduct. The use of Trust email accounts for personal use (‘sign ups’), should not be used as this increases the risks of network account details being compromised through cyber-attacks and data leaks of third-party organisations.

3.3. Network users should not make derogatory remarks in e-mails about other Trust stakeholders or Trust/academy competitors or any other persons. Any written derogatory remark may constitute libel.

3.4. Network users may want to obtain confirmation of receipt of important messages. Network users should be aware that this is not always possible and may depend on the external system receiving your message. If in doubt, telephone to confirm receipt of important messages.

3.5. By sending messages on the Potteries system, users are consenting to the processing of personal data contained in that e-mail. If users do not wish the Trust to process such data, they should communicate it by other means.

3.6. The Potteries Microsoft 365 tenancy automatically appends the following statement to all outgoing external e-mail messages which use the system:

This message (and any associated files) is sent in confidence for the addressee only. It may contain confidential or sensitive information. The contents are not to be disclosed to anyone other than the addressee. Unauthorised recipients are requested to preserve this confidentiality and to advise us of any errors in transmission. Any views or opinions expressed in this e-mail are those of the sender and do not necessarily coincide with those of our academy or the Potteries Educational Trust.

3.7. The Potteries network blocks all potentially executable e-mail attachments. Since these types of files potentially constitute the most severe virus attack. Files with the following extensions are currently banned, *.exe, *.bat, *.vbs, *.com. This list is not exhaustive, and the Trust reserves the right to block other types as and when necessary, including the exclusive use of designated wireless networks.

3.8. Reasonable private use of the Internet is permitted but should be kept to a minimum and should not interfere with your work. Excessive private use of the Internet during working hours may lead to disciplinary action and may in certain circumstances be treated by the Trust as gross misconduct, however, this may vary at each individual academy level. The Potteries network and designated IT Team can perform tracks on usage and filters all outgoing and incoming internet traffic.

3.9. The Trust reserves the right to withdraw at any time access to social networking sites or personal blogs on the individual academy managed networks.

3.10. The Potteries network monitors all Internet access and blocks sites with unsuitable content. Network users may bypass this security to facilitate better access – the user has responsibility to ensure that the sites accessed are appropriate. Network users should not assume that just because a site is not blocked that the Trust does not consider it unsuitable. The sites accessed must comply with the restrictions set out in this document. Accessing inappropriate sites may lead to disciplinary action. The Trust expects all academy network users to report any inappropriate sites through the relevant IT Support channels to allow sites to be blocked.

3.11. Managers/teachers do not have automatic rights to access a staff/student member's mailbox. If the manager or a colleague needs access to retrieve a document (when the mailbox owner is absent or on leave) this can be facilitated but IT will need precise details of the document/message that needs to be found. The entire process will be recorded and, in all cases, reasonable attempts to contact the owner to advise them of the action being taken will be carried out. Requests need to be made via IT Helpdesk tickets, but this does not guarantee the request will be actioned

3.12. If unacceptable use of Potteries email needs investigating, it must be discussed with the HR and/or Senior Management from the academy as part of any investigatory process. This must be carried out prior to contacting IT. In such circumstances a check will only take place (without first gaining permission from the mailbox owner) if either the Trust IT Management Team and/or the Trust Exec Group feel that it is necessary. Such circumstances would be exceptional.

4. User Accounts

4.1. Users of the Potteries network receive a 50GB mailbox and a 1TB OneDrive by default. If extra space is needed it can, in exceptional circumstances, be allocated.

4.2. On leaving the Trust it is the user's responsibility to ensure that any documents are transferred as appropriate in line with individual academy procedures

4.3. A user network area/OneDrive is primarily for storing items that relate to Trust and/or academy work; it is not for personal use. Using this area to store personal items may lead to disciplinary action.

4.4. All network users, who access information and data offsite, including access to Microsoft 365, are required to have their account protected with multi-factor authentication (i.e. not at academy locations).

4.5. To support data protection compliance, all network users must use the screen-lock functionality of the device when or if they leave a device unattended.

4.6. Users must be logged off if there is no plan to return to the device, including overnight to avoid losing any unsaved work.

4.7. Users are required to restart their device on the Potteries network at least once a week to receive the latest patches and policy updates.

5. **Copyright Infringement**

5.1. Copyright applies to all text, pictures, video, and sound, including those sent by e-mail or on the Internet. Files containing such copyright protected material may be downloaded, but not forwarded or transmitted to third parties without the permission of the author of the material or an acknowledgement of the original source of the material, as appropriate.

5.2. Copyrighted software must never be downloaded. Such copyrighted software will include screen savers.

5.3. The maximum file size permitted to be downloaded equals the allocated amount of network area specified above (User Accounts 4.1).

5.4. Users of the computing facilities should not import non-text files or unknown messages on to the Potteries network system without having them scanned for viruses.

5.5. Users of the computing facilities must never engage in the political discussions through outside newsgroups using the Potteries e-mail system or its network.

6. **General Computer Usage**

6.1. Users are responsible for safeguarding their passwords for the system. For reasons of security, individual passwords should not be written down, printed, stored on-line, or given to others.

6.2. Due caution should be given when opening emails that ask for network credentials or contain links to unknown websites

6.3. Users should change their password immediately if they suspect their password has been compromised and contact their academy IT Support.

6.4. Passwords should follow the current Trust password standards which will be in line with current national cyber security advice and guidance.

6.5. Ability to connect to other computer systems through the network does not imply a right to connect to those systems or to make use of those systems unless authorised to do so. Users should not alter or copy a file belonging to another user without first obtaining permission from the creator of the file.

6.6. Installation of Software should under no circumstances, be undertaken by network users. Only designated personnel may install software. Installing unauthorised software may lead to disciplinary action and may in some circumstances be treated as gross misconduct. This includes all Potteries network locations, including the use of the 'off-network' dedicated TLAB environment. Users of the TLAB will adhere to this Acceptable Use Policy.

6.7. Employees of the Trust will be subject to the rules and regulations laid down in the Potteries Educational Trust's policies and procedures relating to GDPR and Information Security

6.8. If the Internet facilities are used for personal use, such as purchasing goods with a credit card, users do so at their own risk. The Trust accepts no responsibility for any personal transactions carried out over the Potteries network.

6.9. The Potteries Guest Wi-Fi networks exist to give visitors Internet access as a free service, connecting to this network with own devices is at the user's risk. The Trust accepts no responsibility for damage to personal devices caused by any sites visited or material downloaded.

6.10 Network users, who use their personal devices must use the eduroam wireless network.

6.11. The Potteries network supports the use of personal devices at the Sixth Form College through dedicated Wi-Fi networks; however, all members of the Trust community are expected to ensure the personal device is:

- regularly updated for both operating systems and software packages, including security patches within a 14-day release period.
- in scope for support from the vendor.
- used to access academy data using approved application only.
- free from malware/malicious software and has appropriate anti-virus protection installed configured to scanned daily with real-time file scanning.
- setup to enable for web page scanning as part of anti-malware protection software.
- free from illegally obtained software including peer-networking software.
- set up with password and/or PIN in line with the Trust's password procedure document (which is currently ten characters with Microsoft's password complexity requirements enabled).
- free from software no longer required.
- set up with only the necessary user accounts on your personal device.
- set up only contains signed applications that have been verified and installed from the corresponding vendor App Store.

7. Section A : Trust Portable Devices – Laptops, Mobile Phones, iPads, VR/AR & Immersive Technologies

7.1. Users of Trust mobile and portal devices must be vigilant in caring for their security. If a device is stolen, the user is expected to report the theft to the police, obtain an incident number and contact academy level IT Support as soon as possible.

7.2. Users of Trust devices must not change technical settings or interfacing configuration with laptops or other equipment without first consulting IT Services. Users who alter the configuration of a device, may be liable to compensate the Trust for any losses.

7.3. Users who borrow loan equipment are required to sign for it and bear the responsibility for its care. Loan equipment should be concealed and stored securely when not in use and returned per the appropriate loan arrangements

7.4. Users of the Trust mobile devices (including VR Headsets, Immersive Technologies, and other recording facilities) are required to follow the guidance of the supporting academic or professional services staff within each academy.

Section B : Student Portable Devices

7.5. Users of student laptops provided through any institutional leasing scheme or otherwise, must report lost or stolen devices to their local ICT Support department.

7.6. Users of Trust devices must not change technical settings or interfacing configuration with laptops or other equipment

7.7. Users who borrow loan equipment are required to sign for it and bear the responsibility for its care

8. Social Media

8.1. The Potteries network internet service is provided for the use of the Trust's official business and as a teaching and learning resource, but the Trust recognises that many use the internet for personal purposes, and that many participate in social networking on websites such as Facebook and Twitter - the level of access permitted and deemed suitable will be managed at each academy. However, all members of the Trust and wider community are expected to always set the highest professional standards, both in and out of each academy, in order that the Trust achieves its mission that its users have a safe learning environment for their students. We also expect users to create separate social media accounts solely for Trust and/or academy use giving clear separation between personal and business accounts.

8.2. During any use of social networking sites or maintenance of personal blogs (online diaries), network users are required to refrain from making any references to the Trust and/or any of its academies that could bring it into disrepute or interacting or writing on the sites in a way that could constitute harassment of a colleague, student, or employer. The Trust may treat any breaches of these requirements as disciplinary offences.

8.3. All network users must take care not to allow their interaction on these websites to damage working relationships between other members of the Trust and wider academy-level community. Postings to newsgroups social network sites are in effect e-mails published to the world at large and are subject to the same regulations governing email as above. It is expected that disclaimers are used with a posting if it could be interpreted as an official statement or policy of Potteries Educational Trust. For example: "The views expressed are my own and do not necessarily represent the views or policy of the Potteries Educational Trust or any of its academies... " If a user makes a remark or is responsible for or in any way involved with posting material which in the opinion of the Trust and brings the Trust and/or an academy into disrepute or otherwise damages the Trust’s interests, disciplinary action may also be taken in line with the academy's appropriate disciplinary policy. Any legal means may be taken to search accessible materials relating to the disciplinary action.

8.4. Extreme care must be taken if it is necessary to provide endorsements about members of the Trust community, and personal comments about any stakeholders are not acceptable. If in any doubt about other specific usage of site(s) then discuss the matter with your Academy Management Team or Middle Manager, in the case of students, your Progress Coach or Form Tutor.

8.5. Network users must also be security conscious and should take steps to protect themselves from identity theft, for example by restricting the amount of personal information that they give out. In addition, users should ensure that no information is made available that could provide a person with unauthorised access to the Potteries Network and/or any confidential information; and refrain from recording any confidential information regarding the Potteries Educational Trust on any social networking website. Care should always be taken to ensure that information provided to such sites does not contravene our Data Protection Policy.

Implementation

A copy of this policy will be provided to all student's, employees, consultants, contractors, and volunteers who will be provided with access to Potteries network.

In any case where there is clear infringement of the Acceptable Use Policy ICT Services and/or Academy IT Support will be guided by the Human Resource/ Senior Management Teams in any action that needs to be taken against the infringer.

Communication

- Information to be shared with Network users; through Induction, Staff Briefings or via Email Notices. Students will have access to relevant information and/or documents through Tutorials or through academy level sessions and platforms.

Monitoring

- Impero/or alternative implementation of AUP on user logons with *electronic signatures* required on a termly basis to cover changes to policy or capture new starters, including staff and/or students.

Associated Information and Guidance

- Review of Policy in line with Cyber Essentials requirements for Potteries Educational Trust.
- If there is any part of this document you do not fully understand, contact any Trust IT Management Team, or localised academy IT Support, who will be happy to explain the issue in greater detail.

Related Documents

- PET IT Security Policy.
- PET Data Protection Policy