Acceptable IT Use & Data Protection Policy

Policy Family	Information Governance
Responsible Manager	Trust Director of IT / COO
Approval Date	October 2025
Issue Number	1.0
Review Date	October 2026

1. Aim

Acceptable Use of IT, Technology, Systems and ensuring compliance with GDPR legislation.

This IT Code of Conduct sets out the standards of behaviour expected for all users of the Potteries Educational Trust IT networks, systems, and devices. This policy applies to staff, students, trustees, governors, contractors, consultants and external users.

The purpose of this policy is to:

- Ensure safe, secure, and responsible use of IT resources.
- Protect the integrity of the Trust's IT infrastructure, data, and reputation.
- Support compliance with statutory requirements, including the Department for Education (DfE) standards, the UK General Data Protection Regulation (GDPR), the Data Protection Act 2018, and the Cyber Essentials Framework.
- Safeguard all users.

2. Scope

This policy applies to all use of:

- Trust-owned or leased devices (e.g., laptops, tablets, desktops, servers, interactive screens, printing and telephony technology).
- Personally-owned devices accessing Trust services (Bring Your Own Device – BYOD).
- Internet and email services provided by the Trust.
- Cloud-based platforms (e.g., Microsoft 365, Google Workspace, MIS, VLEs and any other third-party Software Solutions).
- Trust networks, Wi-Fi, and remote access systems.

3. Responsibilities

- All Users must read, sign, and follow this IT Code of Conduct.
- Senior Leaders, Trustees, and Governors must ensure oversight of IT use and compliance.
- IT Services must implement and monitor technical controls in line with Cyber Essentials.
- Working with the Trust IT Team, Safeguarding Leads will ensure appropriate filtering, monitoring, and reporting in line with Keeping Children Safe in Education (KCSIE) has been implemented at localised Academy Level.

4. Acceptable Use

4.1 General Principles

- Use IT resources responsibly, respectfully, and lawfully.
- Protect account details. Passwords must never be shared.
- Meet National Cyber Security Guidance on Password recommendation and strength. *Guidance available through IT Helpdesk Function.*
- Report suspected security incidents, breaches, or safeguarding concerns immediately.
- Access only systems, data, and information authorised to use.
- Follow guidance and update device with latest patches within 14 days to meet Cyber Essentials requirements.

4.2 For Students (*All Educational Settings* – Primary/Secondary/Sixth Form/College/Foundation Degree)

- Use IT and internet access only for learning, research, and educational purposes.
- Always follow staff instructions regarding online platforms and digital tools.
- Treat others with respect when communicating online.
- Do not attempt to bypass internet filtering, monitoring, or security controls.
- Never share personal information (address, phone number, passwords) online.
- No installation of software on Devices, unless approved or made available through the Trust Software Portal.

4.3 For Staff

- Use IT systems for educational, administrative, and professional purposes only.
- Ensure personal devices used for Trust purposes comply with security requirements (password protection, encryption, updated software).
- Follow data protection requirements when accessing, storing, or sharing information.
- Lock or log off devices when unattended.
- Use only Trust-approved platforms for communication with students and parents/carers.

4.4 For Trustees and Governors

- Access systems only through secure, authorised channels.
- Treat all governance documents and communications as confidential.
- Do not download or store Trust information on personal, unencrypted devices.

4.5 For Guests and Contractors

- Access the Trust network only through designated guest Wi-Fi or approved accounts.
- Use is restricted to legitimate educational or business purposes.
- All use is subject to monitoring and this policy.

4.6 Social Media Use

The Trust recognises the value of social media for communication, collaboration, and professional development. However, all use of social media by staff, students, trustees, governors, and guests must be responsible, lawful, and aligned with the ethos of the Trust as per *PET Social Media Policy*.

- ➢ On Trust-owned Devices and Networks
  - Social media may only be accessed for educational or professional purposes, unless otherwise authorised.

  - Use must not disrupt learning, teaching, or work responsibilities.
  - Only Trust-approved accounts and platforms may be used for official communications.
- On Personally-owned Devices (BYOD or outside the Trust)
  - Personal use of social media outside Trust systems must not bring the Trust into disrepute.
  - Users must not post content that:
    - Identifies the Trust, its schools, staff, or students in a negative, offensive, or defamatory manner.
    - Discloses confidential or sensitive information.
    - Breaches safeguarding responsibilities (e.g. inappropriate contact between staff and students).
  - Staff must maintain appropriate professional boundaries online (e.g. no "friending" or direct messaging with students on personal accounts).
  - Trustees and Governors must ensure that any online commentary aligns with their governance responsibilities and maintains the Trust's reputation.
  - Students must follow the Trust's behaviour policy in relation to online activity, including off-site use where behaviour impacts the school community.

5. Prohibited and Unacceptable Use

The following activities are strictly forbidden. These examples are not exhaustive; any behaviour that breaches Trust policy, statutory guidance, or the law will be treated as a breach of this policy.

- Sharing passwords or using another person's login credentials.
- Attempting to gain unauthorised access to systems, accounts, or data.
- Installing unauthorised or unlicensed software on Trust devices.
- Using unapproved USB sticks or external drives without encryption.
- Attempting to bypass security controls, such as firewalls, web filters, or monitoring systems.
- Using Trust networks or devices for illegal file sharing, streaming, or gaming.
- Deliberately introducing viruses, malware, or other harmful code.
- Sending or forwarding chain letters, spam, or junk mail.
- Posting negative, offensive, or defamatory comments about the Trust, its schools, staff, students, or community (even on personal accounts).
- Engaging in cyberbullying, harassment, or online abuse.
- Uploading, downloading, or sharing copyrighted media illegally.
- Recording or sharing images/videos of staff or students without permission.
- Using Trust email or systems for personal business, secondary employment, or political activity.
- Accessing or distributing extremist, pornographic, or discriminatory material.
- Attempting to log in from outside approved geo-locations using unauthorised methods.
- Disabling or refusing to use MFA.
- Sharing MFA tokens, one-time codes, or authenticator access with others.
- Accessing Trust systems using anonymisers, VPNs, or proxy services not approved by IT.

This list is not exhaustive.

6. Security, Data Protection, Copyright & Access Controls

6.1 Security and Access Controls

- Multi-Factor Authentication (MFA) is mandatory for all Trust Staff, Post 16 Learners, Trustees, and Governors.

- Multi-Factor Authentication (MFA) is implemented for Primary School Learners with Geo-Location to restrict active logons to within the school premises or wider Trust Network only.
- Multi-Factor Authentication (MFA) is currently optional for Secondary School Learners, with a future implementation to be considered by Trust Senior Management. However, Multi-Factor Authentication maybe enforced for 'High-Risk' users as identified by Microsoft 365 Defender.
- MFA must be configured and used on all Trust accounts (utilising Microsoft 365 SSO).
- Geo-location Conditional Access is in place to protect the Trust's cyber posture. Logins from outside the UK or from unusual locations may be blocked, restricted, or require additional verification.
- Multi-Factor Authentication (MFA) will not be required within Academy locations when within the Trust network.
- Devices accessing Trust systems must comply with security requirements (latest updates, antivirus, strong password protection).
- Lost, stolen, or compromised devices must be reported immediately to local Academy IT Services.

6.2 Data Protection (GDPR)

All users must adhere to UK GDPR and Data Protection legislation; any updates or changes to legislation will be communicated through the Academy's official channels, and users are expected to comply accordingly.

- Personal data must only be accessed or shared via encrypted, Trust-approved platforms.
- Users must not transfer personal data to unencrypted personal devices or unauthorised cloud storage.
- All staff must comply with the Trust's Data Protection Policy and GDPR requirements

6.3 Data Breaches and Reporting

A personal data breach is any incident resulting in accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

****Examples:****

Sending an email with personal data to the wrong recipient.

- Losing an unencrypted device containing Trust data.
- Accidentally making personal data publicly accessible online.
- Hacking, malware, or phishing leading to unauthorised access of a Trust account(s).

This list is not exhaustive.

****User Responsibilities:****

- All staff, trustees, governors, and students must immediately report any suspected or actual data breach to the Trust's Data Protection Officer (DPO) via the Trust's reporting procedure (dataprotection@potteries.ac.uk).
- Users must not attempt to conceal breaches or handle them independently.
- Staff should inform their line manager.
- DSL should be informed if the breach has safeguarding implications.
- The Trust will investigate and record breach to external Data Protection Service (SchoolPro) via Academy Data Protection lead.
- Trust Senior Management will report notifiable breaches to the ICO within 72 hours. The Chair of the Audit and Risk Committee Board will be informed.

6.4 Copyright & Intellectual Property

- Users must respect copyright, licensing agreements, and intellectual property rights.

- Downloading, sharing, or using unlicensed or pirated material (e.g., films, music, software, games, textbooks) is prohibited.
- All work, resources and documentation created, stored, or transmitted on Trust systems or devices are the intellectual property of the Trust and not the individual author, unless otherwise agreed in writing by the Trust.
- Educational exemptions must be used responsibly and in line with Trust guidance.

7. Safeguarding & Online Safety

- The Trust uses Smoothwall, a robust filtering and monitoring system, to identify and highlight risks associated with websites and online activities accessed by both staff and students.
- Alerts are reviewed by authorised staff, who will take appropriate action where concerns arise.
- Filtering and monitoring always apply when using Trust networks and devices. Attempts to bypass or disable these systems are strictly prohibited.
- Students will receive age-appropriate filtering categories to ensure safe and responsible internet use.
- Staff will receive appropriate filtering on devices ensuring safe and responsible internet use.

8. Use of Microsoft 365 (Email, OneDrive, SharePoint and Teams)

- Email accounts are provided for Trust-related communication only. Personal use must be minimal.
- Users must check Trust email accounts regularly to stay informed.
- Use Trust email (not personal) for official communication with students, parents/carers, and colleagues.
- Users should not attempt to send or share executable email attachments (e.g. .exe, .bat, .reg, .vbs).
- Use professional language and subject lines. Emails may form part of official records.
- Use BCC when emailing groups to protect personal data.
- Attachment must be reviewed prior to being sent. Trust IT recommends using SharePoint links to share documentation rather than attachments to revoke future access from emails, once sent.
- Do not send sensitive data by email unless encrypted/password protected.
- Do not open attachments or click links from unknown senders; report immediately to Spam Report Mailbox. (spamreport@potteries.ac.uk).
- Staff & Students must use email only for learning purposes, communicate respectfully, and not use Trust email for social media or sign-ups.
- OneDrive, Teams and SharePoint should only be primarily used for storing items that relate to Trust and/or academy work.

9. Monitoring and Privacy

- The Trust reserves the right to monitor, access, and review network usage, emails, and online activity for compliance, safeguarding, and security purposes.
- Users should have no expectation of personal privacy when using Trust systems.

10. Breach of Policy

Breaches of this Policy may result in disciplinary action, removal of access, and/or legal action.

- For students: sanctions in line with the Behaviour Policy.
- For staff: disciplinary action up to and including dismissal.
- For Trustees/Governors: removal from office in line with governance codes of conduct.
- For guests/contractors: withdrawal of access and termination of contracts.
- Serious breaches may be referred to external agencies (police, LADO, ICO, DfE), as appropriate.

Implementation

Implementation of this policy and procedures will be the responsibility of the Trust Director of IT, supported by Line Managers and Senior Managers who will act on behalf of the Trust in all matters related.

All users must confirm that they have read, understood, and agreed to comply with this Policy before accessing the Trust's IT networks and systems.

Electronic e-signatures will be prompted by all users prior to their first use of the Trust Computer Network. Alternative signatures will be done for accounts used outside of the network.

Communication

This Policy will be circulated to appropriate staff within the Trust and is also available from the central policy area.

Monitoring

The responsible manager named on the front of this policy is responsible for ensuring that this document is kept up to date and revised as appropriate in line with legislative changes, seeking management and/or trustee approval in advance of the review date so that a new version can be communicated to employees in a timely fashion.

This policy will be reviewed annually, or earlier if required, in line with statutory guidance, DfE standards, and evolving cyber security best practice.

Related Statutory Rights and Policies

- Data Protection Act 2018 & UK General Data Protection Regulation (UK GDPR)
- Cybersecurity Guidelines (e.g., NCSC Guidelines)
- Computer Misuse Act 1990
- Keeping Children Safe in Education (KCSIE) 2025
- Equality Act 2010
- Public Sector Bodies (Websites and Mobile Applications) Accessibility Regulations 2018
- Health and Safety at Work Act 1974
- Children's Privacy and Data Rights (ICO Children's Code)
- Meeting digital and technology standards in schools and colleges (2024)
- Academy Trust Handbook 2024