Pathway Trust

Acceptable Use of IT Policy

Policy effective from	21 September 2026
Policy owner	Director of People
Policy applies to	Berrow Church Primary School Burnham-on-Sea Infant School Castle Batch Primary School Charfield Primary School Cherry Garden Primary School Downend School East Huntspill Primary School Lyde Green Primary School Mangotsfield School Marlwood School Pawlett Primary School Priory Community School Severn Beach Primary School St Andrew's Church Junior School St Anne's Church Primary School The Castle School The King Alfred School Tortworth Primary School West Huntspill Primary School Worle Community School Pathway Partnership Teams
Policy changes since last version	New policy

1. Introduction

1.1. Technologies and the internet are powerful tools which provide excellent opportunities for learning and teaching. They can motivate learners, promote creativity, and support effective learning, assessment and engagement.

1.2. Pathway Trust provides computer equipment for use by employees as an important tool for teaching, learning, and administration of the trust/school.

1.3. Employees have a responsibility to use the trust's computer systems and equipment in a professional, lawful, and ethical manner and its use is governed by the following policy.

1.4. Please ensure you understand your responsibilities under this policy, and direct any questions or concerns to the Head of IT in the first instance. Any breach of this policy may result in disciplinary or other action.

1.5 This policy supports compliance with UK GDPR and relevant Department for Education guidance and helps protect the trust's data, systems and reputation.

2. Scope

2.1. The policy applies to all employees regardless of length of service including those in their probationary period. It also applies to agency workers, self-employed workers, members, trustees, community councillors, contractors, trainees, secondees and visitors. For the purpose of this policy the term 'employee' is used throughout.

2.2. It is intended to ensure that:

- Users stay safe while using technologies;
- The trust IT systems and users are monitored to ensure protection from accidental or deliberate misuse that could put the security of the systems and users at risk;
- Employees are protected from potential risk from the use of IT in their everyday work and work to ensure that young people in their care are safe users;
- The trust is protected from any issues that could negatively affect its reputation.

3. Use of Trust ICT Equipment and Software

3.1. The trust provides a range of ICT equipment and software for employees. That includes, but is not limited to:

- Computers, tablets, mobile phones and other devices.
- Access permissions for certain programmes or files.

3.2. Single Sign On or Multi-factor authentication will be enabled for any software accessed via the internet (Software as a Service - SaaS).

3.3. Employees are not permitted to purchase or install any ICT equipment or services and software without prior authorisation from the Director of Finance, the Head of IT and for software contact the HR Services Manager so that a Data Protection Impact

Assessment (DPIA) can be carried out. This is to ensure that it is compatible, licences are compliant and any wider implications are considered.

3.4. The trust will provide access to ICT equipment for use on site and remotely. Employees are responsible for ensuring the security of IT equipment assigned to them.

3.5. ICT Equipment must be logged off or locked when the employee is away from their desk. Laptops must be locked away when not in use, preferably in a lockable cupboard and any equipment taken off site should be carried in a suitable bag, remain in the employees possession, secure and out of sight at all times.

3.6. Employees will be provided with their login/account information and passwords which must be used when accessing the trust's ICT systems.

3.7. Passwords and usernames must not be written i.e. in office diaries or disclosed to anyone, other than the trust IT Services who are responsible for running and maintaining the trust systems. Passwords must be immediately changed if an employee believes their password(s) may have been compromised or if instructed to do so by the system or the trust IT Services.

3.8. Employees must not disclose passwords or usernames to anyone other than authorised trust IT Services personnel.

3.9. Employees must never allow a pupil to use their login credentials or account for any reason.

3.10. In the event of gaining access to files that an employee is not authorised to view or edit, or where access permissions need to be amended, employees should contact the IT Service Desk.

3.11. The use of personal email addresses for work related materials or business is prohibited, and employees must never disclose their personal email addresses and personal mobile phone numbers to parents/carers and pupils.

3.12. Any assets (electronic data or otherwise) created during employment with the trust remain the property of the trust, during and at the end of employment. The continued use of any trust assets (e.g. learning resources) in another setting or context once employment has terminated requires prior authorisation from the Headteacher/Director.

3.13. All physical trust assets, including devices, chargers and other peripherals, must be returned immediately when employment or engagement ends. Access to trust systems will be revoked in line with the trust's leaver process.

3.14. The trust uses remote monitoring and investigation tools and employees are reminded this includes email, browsing history and stored files for the purposes of safeguarding and data protection.

3.15. The use of Generative AI is permitted; however employees must not upload or transmit sensitive or personally identifiable information into public AI.

3.16. Employees will need to attend mandatory Cyber Security training annually as part of our Cyber Security compliance.

4. Use of a Pathway Trust Email and other electronic communications

4.1. Employees will be provided with a trust email address which should be used to conduct all work-related correspondence.

4.2. Single Sign On or Multi-factor authentication will be enabled on the trust email account.

4.3. Care must be taken to ensure:

- Email messages do not include incorrect or improper statements which can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.
- Attachments containing sensitive or confidential information are encrypted so that the information is only accessible by the intended recipient.

4.4. Email messages are required to be disclosed in legal proceedings or in response to requests under the Data Protection Act 2018 and the Freedom of Information Act 2000 in the same way as paper documents. If an email is deleted from an inbox, it does not mean that an email cannot be recovered for the purposes of disclosures. All email messages should be treated as potentially retrievable.

4.5. If an email is sent or received in error, it must be reported through the School Operations Manager to the trust's Information Governance Manager at dataprotection@pathwaytrust.uk so that the data breach procedures are invoked immediately.

4.6. Employees can set a profile image/avatar to their trust email address. They must be professional and representative of an employees' likeness. Anything other than a photo of the employee will be removed.

4.7. Emails received with attachments should only be opened if the email has come from a trusted source and/or it was expected.

5. Use of a Digital Communications

5.1. Trust mobile phones are provided to employees dependent on their role and are intended for the use of work-related matters only. They must only be used for personal use in exceptional circumstances.

5.2. Trust mobile phones and other managed mobile devices must be enrolled in and controlled through the Trust's approved mobile device management service.

5.3. When communications are made externally via telephone or video conferencing employees should take account of their environment and refrain from using loudspeaker or hands-free devices in public spaces, as there may be reference to personal or special category information.

6. Personal Use of ICT Equipment

6.1. Employees are permitted to occasionally use trust ICT equipment and facilities for personal use.

6.2. Personal use is permitted provided that such use:

- Does not constitute 'unacceptable use' as outlined in Section 8.
- Does not take place when pupils are present.
- Does not interfere with undertaking their role or prevent other employees or pupils from using the facilities for work or education purposes.
- Does not include the storing of information or materials (such as music, videos or photos).

6.3. In the event of this permission being overused or abused, the Headteacher/Director may withdraw or restrict permissions at any time.

7. Online Access to Information

7.1. Employees can access trust ICT equipment and facilities remotely and must abide by the same rules as accessing ICT onsite. Employees must be aware of their surroundings and remain vigilant ensuring precautions are taken as prescribed by the trust IT Services to avoid importing viruses or compromising system security.

7.2. The trust ICT systems contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with the trust's Data Protection Policy.

7.3. When working remotely (including using any form of video conferencing and making or receiving telephone calls), employees should take account of the environment and be aware of what may be able to be seen or heard through the computer or telephone and ensure that the device is appropriately locked or logged off. This includes accessing work emails on a personal device or telephone.

7.4. Where a personal device is permitted to access trust data or services, the device must:

- Be protected by a passcode, PIN or equivalent secure authentication.
- Use device encryption.
- Be capable of remote wipe, with the employee consenting to remote removal of Trust data where required.

8. Unacceptable use

8.1. The following is considered unacceptable use of trust ICT:

- Using trust ICT to breach intellectual property rights or copyright.

- Using trust ICT to bully or harass someone else, or to promote unlawful discrimination.
- Breaching trust policies and procedures.
- Any illegal conduct, or statements which are deemed to be advocating illegal activity.
- Online gambling, inappropriate advertising, phishing and/or financial scams.
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful.
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/livestreams.
- Activity which defames or disparages the trust, or risks bringing the trust into disrepute.
- Sharing confidential information about the trust/school, its pupils, or other members of the school community.
- Connecting any device to the trust ICT Network without approval from ICT Services.
- Setting up any software, applications or web services on the trust network without approval by trust IT Services or creating or using any programme, tool or item of software designed to interfere with the functioning of the trust ICT, accounts or data.
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval.
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to trust ICT.
- Causing intentional damage to trust ICT.
- Removing, deleting or disposing of trust ICT, systems, programmes or information without permission.
- Using inappropriate or offensive language.
- Promoting a private business, unless that business is directly related to the trust/school.
- Using websites or mechanisms to bypass the trust's filtering or monitoring mechanisms.
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way.

- Damaging computer equipment and or loosing equipment assigned to an employee. In this event, damage not considered 'wear and tear' may be charged to the employee.
- Making a copy or transfer any data to storage systems other than the trust network or equipment provided by the trust for business use. This includes USB memory sticks and external hard drives (even those owned or issued by the trust), cloud storage (non-trust) or a personal computer.
- The use of electronic devices (including personal and trust mobile phones, smartwatches, cameras, and USB drives) are prohibited in areas where live or sensitive examination materials are stored, prepared, or administered.

8.2. This list is not exhaustive. The trust reserves the right to amend this list at any time. The Headteacher/Director will use their judgement to determine whether any act or behaviour not on the list is considered unacceptable use of IT.

9. Use of Images, Video and Pupil Data

9.1 Personal devices must not be used to photograph or video pupils.

9.2 When using a trust device, employees must verify that the appropriate parental or carer consent is in place before publishing or sharing images or video of pupils.

9.3 Further requirements are set out in the Trust Code of Conduct and relevant safeguarding and data protection policies.

10. Reporting Incidents

10.1. Any incidents must be immediately reported to the IT Service Desk. Examples include:

- Receipt of a suspected virus or in the event of experiencing any unusual occurrences (e.g. an antivirus software warning, pop-ups without the browser open, unable to open files or task manager).
- Any suspected or observed security breach.

11. Breach of the policy

11.1. Deliberate abuse of the trust's computer systems and breaches of this policy may be dealt with under the disciplinary procedure, and civil and/or criminal liability.

12. Review

12.1. This policy is reviewed every year by the trust. We will monitor the application and outcomes of this policy to ensure it is working effectively.