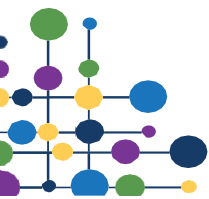




ICT POLICY & PROCEDURE

MAT Version	3.0
Name of Policy Writer	Z Iqbal
Approved by Directors or Delegated Authority	07.09.26
Date of next review	April 2027

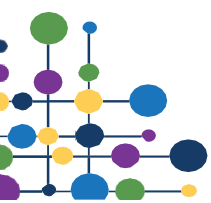




SHARE MAT ICT Policy and Procedure

Contents

1. Introduction
2. Purpose
3. Scope
4. Governance and Responsibilities
5. ICT Service Management
6. Cyber Security
7. Safeguarding and Online Safety
8. Identity and Access Management
9. Asset Management
10. Software and Licensing
11. Data Protection and Information Management
12. Backup and Disaster Recovery
13. Acceptable Use of ICT
14. Email and Communication
15. Remote Working and Mobile Devices
16. Social Media
17. Personal Devices (BYOD)
18. Trust Wi-Fi and Network Access
19. Incident and Breach Management
20. Training and Awareness
21. Monitoring and Compliance
22. Continual Improvement
23. Photographs and Photography
24. Artificial Intelligence (AI) and Generative AI Usage
25. Schedule of Amendment





1. Introduction

SHARE Multi Academy Trust is committed to the effective, safe and secure use of ICT and digital services to support teaching, learning, communication and operational excellence across all schools and central functions.

The Trust recognises that digital services are essential to curriculum delivery, safeguarding, business continuity, governance, collaboration and inclusion. This policy sets the standards for how ICT services are governed, delivered, secured and used.

The Trust aims to provide a modern and resilient digital environment in which staff and students are confident, responsible and secure users of technology.

2. Purpose

This policy defines how ICT services are delivered, supported, secured, monitored and used across the Trust.

It establishes clear expectations for users, leadership and the IT service, and supports compliance with UK GDPR, the Data Protection Act 2018, Keeping Children Safe in Education (KCSIE), DfE Digital and Technology Standards and recognised NCSC cyber security good practices.

The policy is intended to reduce risk, support safeguarding, protect data, improve service quality and enable continual improvements to Trust systems and ICT procedures.

3. Scope

This policy applies to anyone who uses or accesses Trust systems, devices, networks or cloud platforms, including staff, students, governors, trustees, trainees, volunteers, contractors, agency workers, consultants, visitors and temporary staff.

It covers all ICT and digital services the Trust owns, manages or uses, including networks, servers, endpoints, Microsoft 365 services, internet access, wireless networks, telephony, software, applications and approved third-party platforms.

The policy applies whether access is on site, remote or through approved personal devices.

4. Governance and Responsibilities

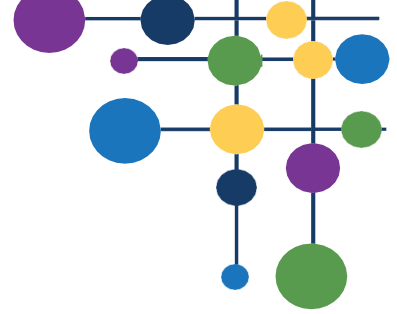
The Trust is responsible for ensuring ICT supports education, safeguarding, operational effectiveness and legal compliance. It must also maintain appropriate governance, risk management and resources to manage ICT services effectively.

The Trust will maintain a risk management process of a formal cyber risk assessment conducted at least annually and reviewed at least termly. Identified risks will be recorded, assessed for likelihood and impact, and managed through appropriate technical, organisational and procedural controls. Significant risks will be escalated through Trust governance arrangements in line with risk management processes.

The IT service is responsible for delivering services, maintaining cyber security controls, managing assets and configurations, responding to incidents, maintaining systems, improving services and providing technical assurance.

Headteachers, senior leaders and line managers must ensure staff follow this policy in practice, adhere to local procedures and escalate serious issues without delay.





All users must use systems safely and professionally, protect devices and data, and report faults, concerns, incidents or suspected breaches promptly.

5. ICT Service Management

The Trust will manage ICT services in line with recognised best practice, including DfE, NCSC and ITIL principles, to ensure reliability, consistency, accountability and continual improvement.

All incidents, service requests and access changes must be logged through the Trust's helpdesk so they can be prioritised, tracked and resolved effectively.

All system and service changes must be raised through the helpdesk, risk assessed, approved by the IT Manager and tested before implementation. Unauthorised changes are not allowed.

All ICT issues, faults and equipment damage must be reported using the following escalation process:

1. Every system – Staff must raise an Every ticket for all IT issues to support compliance, tracking and reporting.
2. IT support email – Use only for urgent support. An Every ticket must still be raised.
3. Phone – Use only in emergencies. An Every ticket must still be raised.

Recurring issues will be reviewed to identify root causes, reduce repeat disruption and strengthen system resilience.

6. Cyber Security

The Trust will use a layered, defence-in-depth approach to cyber security. Key controls include secure network design, firewalls, endpoint protection, web filtering, email security, monitoring, patching and vulnerability management.

For this the Trust follows the NCSC 10 Steps to Cyber Security to manage cyber risk. These measures help reduce the likelihood of cyber-attacks and lessen their impact if they occur. The 10 steps are:

1. **Risk management** – Identify the data and systems most at risk and assess the threats to them.
 2. **Identity and access management** – Control who and what can access systems and data.
 3. **Engagement and training** – Build security practices that work for staff and users, supported by clear policies, awareness and regular training.
 4. **Data security** – Protect sensitive data with suitable controls, including relevant policies, anti-malware measures and backups.
 5. **Asset management** – Maintain an accurate register of the Trust's systems, devices and data assets.
 6. **Logging and monitoring** – Monitor systems and networks continuously and review logs for signs of unusual or malicious activity.
 7. **Architecture and configuration** – Design, build and maintain systems securely, apply patches, test controls, and use secure baseline configurations.
- 

8. Incident management – Prepare for cyber incidents in advance through maintained response and disaster recovery arrangements.

9. Vulnerability management – Protect systems throughout their lifecycle using patching, anti-malware, firewalls and appropriate access controls.

10. Supply chain security – Work with suppliers and partners to ensure legal compliance and the secure handling of data shared with third parties.

Cyber risks will be managed proportionately through appropriate technical, administrative and procedural controls to reduce both the likelihood and impact of an attack.

Users must not bypass security controls, install unauthorised software, connect unauthorised devices or take any action that could weaken the Trust's security.

The Trust will maintain arrangements to identify, contain, investigate, recover from and learn lessons from cyber incidents.

The Trust will undertake a formal cyber risk assessment at least annually, with termly review points, to ensure that emerging threats, vulnerabilities and changes to systems or services are identified and managed appropriately. This assessment will influence the ongoing development of cyber security controls and priorities.

7. Safeguarding and Online Safety

ICT services will support the Trust's safeguarding responsibilities through internet filtering, monitoring and secure system design that reduce exposure to harmful, inappropriate or illegal content.

Any concerns about harmful online activity, inappropriate content, cyberbullying, exploitation or other safeguarding risks must be reported immediately and escalated in line with safeguarding procedures.

The Trust does not tolerate cyberbullying of students or staff. Inappropriate, suggestive or abusive messages are prohibited, and anyone found to have sent such messages may face action under the relevant age-appropriate Trust Behaviour and Anti-Bullying policies.

The system blocks websites it identifies as threats. If staff need access to a site for educational purposes, they must contact the IT Manager, who will decide whether access is appropriate. Users must not try to bypass the filtering system.

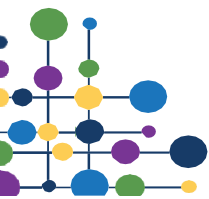
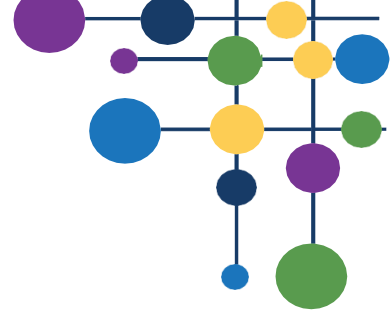
The system monitors and logs the web pages visited, and internet requests made by staff and students. Users should not expect privacy when using the MAT's internet services.

Staff must understand digital safeguarding risks and reflect them appropriately in classroom practice.

Although the filter is robust, some websites may occasionally be misclassified. If a user accesses content unsuitable for a school setting, it must be reported to IT Support immediately so it can be blocked.

The IT team will report any inappropriate, suspicious or illegal online activity by students to the Designated Safeguarding Lead without delay.

The IT team will report any inappropriate, suspicious or illegal online activity by staff, including activity on personal devices connected to the Trust Wi-Fi, to the Headteacher without delay.



Any user who uses the internet inappropriately may have their internet access removed by the Headteacher, who may also take disciplinary action where appropriate.

8. Identity and Access Management

Access to systems is granted based on role, business need and the principle of least privilege. Users will only be given access to the systems, data and functions needed to carry out their responsibilities, as approved by line managers and Headteachers. Privileged access is tightly controlled and subject to additional oversight.

Accounts are created, amended and removed through an authorised onboarding and offboarding process. Access will be updated promptly when staff change roles or leave the Trust.

In line with NCSC guidance, passwords must be 8 to 14 characters long, include uppercase and lowercase letters and special characters, and do not expire. Passwords must be kept confidential and must not be shared. Multifactor authentication is required for all staff, high school and college students using Microsoft 365 and other cloud services.

Staff, high school and college students must use a minimum 14-character passwords. Primary students will be issued with a minimum 8-character passwords. Staff can change student passwords as needed.

9. Asset Management

The Trust will keep an accurate asset register for ICT equipment. Records will identify each asset, its assigned user, location and lifecycle status.

Trust devices, including laptops, iPads, iPhones, ID cards and fobs, remain Trust property and are issued only to authorised users. Users must take reasonable care of equipment, must not move devices without authorisation where location control is required, and must report any loss, damage or theft immediately. All devices must be returned to IT Support when no longer needed or when a staff member leaves.

All laptops and staff iPads are encrypted, receive regular critical and firmware updates, and use anti-virus software that updates automatically when connected to the internet.

Trust devices may be connected to home internet services, but SHARE IT support does not troubleshoot home network issues.

Trust insurance covers theft of hardware and software from Trust premises only. Staff using Trust devices at home should ensure their home and car insurance provides cover for loss or damage.

When working in public, such as on a train, staff must prevent others from viewing sensitive information.

Staff must not repair devices or install hardware or software. Any costs or damage caused by unauthorised repairs or installations may be charged to the designated user.

iPads and iPhones

iPads are single-user devices with persistent logins. Apps such as Safari may retain email logins, Teams access and web history on the device rather than by individual user. Staff must not share assigned iPads, as this may compromise data protection and security. Student iPads are for student use only, and staff must keep a record of who uses them.



10. Software and Licensing

Only approved, licensed and risk-assessed software may be installed or used for Trust business.

Software procurement must consider cost, educational value, cyber security, safeguarding, support, compatibility and data protection.

The Trust uses a standard software configuration across devices, managed centrally through Intune MDM and AppLocker. Installation rights are restricted, and regular checks are carried out to reduce the risk of unlicensed, unsupported or unauthorised software.

Only software covered by a valid individual or site licence may be used on Trust ICT resources. The licence determines whether the software may be used without limit or only on a specified number of devices, and it applies to use on the school site only.

All proposed software purchases and online subscriptions must be discussed with the IT Manager in advance. Once approved and received, they must be registered centrally by the IT Team for secure storage and installation.

Cloud and third-party software must comply with GDPR and cyber security requirements, and multifactor authentication must be enabled where available.

The Trust will carry out regular software audits to ensure no unlicensed software is in use. Records will be maintained of the software installed on each device so licensing compliance can be checked and demonstrated.

Any staff member who suspects unlicensed software is being used must report it to the IT Manager.

Software must not be copied to or from off-site systems unless the licence allows it. Software must not be hired out or sold to another user. Only the IT Manager may install software.

Where staff need software to work from home, the Trust may purchase additional licences. All requests must be approved and monitored by the IT Manager.

11. Data Protection and Information Management

Information must be handled lawfully, fairly and securely. The Trust will apply appropriate controls to protect personal data, confidential information and key operational records.

Users must store information only in approved Trust systems, including Microsoft 365, Arbor MIS and Every for compliance and HR.

Data must be shared on a need-to-know basis using secure methods. Any suspected data breach must be reported immediately.

Only encrypted and approved removable storage devices may be used with Trust devices. The Trust will phase out all removable storage devices during 2026 to 2027.

12. Backup and Disaster Recovery

The Trust will maintain backup arrangements that reflect the importance of its systems and data. These arrangements support service recovery, cyber resilience and business continuity.

The Trust follows a cloud-first approach to storing critical data. Schools use Arbor as their cloud-based MIS, with backups managed by Arbor under the service agreement. All other

school and user data is stored in Microsoft 365 services, including SharePoint, OneDrive and Teams, and is backed up using Barracuda Cloud-to-Cloud immutable backup services hosted in Amazon UK/EU data centres. These arrangements align with DfE backup requirements.

To support business continuity, all critical and operational server systems are virtualised to improve backup and restoration efficiency. These virtual machines are backed up using Veeam, which helps protect systems against loss, unauthorised access, corruption and ransomware-related compromise.

The disaster recovery procedure defines recovery priorities, roles, dependencies and restoration processes for critical services. Recovery processes are tested periodically.

13. Acceptable Use of ICT

Trust ICT systems are provided primarily for educational, professional and operational purposes.

ICT equipment is Trust property and a shared resource. Staff using ICT must:

- not move devices without informing IT;
- check equipment after use;
- leave equipment clean, secure and in good working order;
- switch off equipment, including projectors and interactive boards, after use to save energy and extend its life; and
- not take ICT equipment off site, without permission.

The Trust will monitor use of its ICT systems, networks and services to protect users, investigate misuse, support safeguarding, maintain security and ensure compliance. Users should not expect privacy when using Trust systems.

Users must not access, store, create or distribute inappropriate, illegal, offensive or harmful material, attempt to bypass filtering or security controls, or use ICT in a way that disrupts services or undermines the Trust.

Any software or files downloaded to the Trust network becomes Trust property.

Downloaded software and files must only be used in accordance with their licence terms and copyright restrictions.

Users must not use Trust facilities to download, share or distribute illegal data, illegal software or software that has not been approved by the IT Manager. Any illegal use of MAT resources may result in immediate dismissal.

Downloaded files must be scanned for viruses before they are opened or run. Users must not deliberately spread viruses using MAT internet facilities.

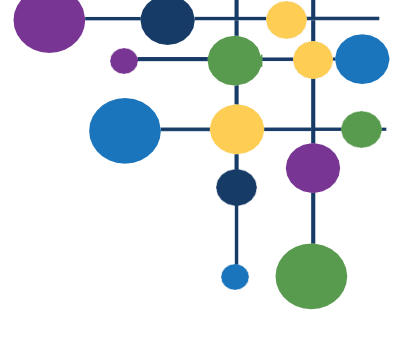
Video and audio streaming or downloading can create significant network traffic and may affect local performance. Downloading video or audio is not permitted unless agreed for demonstration purposes.

14. Email and Communication

Trust-approved systems must be used for Trust business. Communications must be professional, accurate, respectful and appropriate to the context.

Staff must take care when sending personal, confidential or sensitive information, check recipients carefully, and stay alert to phishing, fraud, and unsafe attachments or links.

When using email, staff must:

- 
- avoid using email for emotionally sensitive matters where a face-to-face conversation would be more appropriate;
 - check that recipients are correct before sending;
 - use professional and appropriate language;
 - use CC only where necessary and appropriate;
 - use clear and accurate subject headings;
 - avoid including pupil names in subject lines;
 - manage response expectations clearly; and
 - respond to parent communications within 48 hours.

Microsoft Email and Teams are the Trust's official communication channels for Trust business and must be used to support auditing and compliance.

Personal messaging apps, personal email accounts and informal channels such as WhatsApp must not be used for Trust business where approved Trust systems are available.

15. Remote Working and Mobile Devices

When working remotely, users must use approved systems and security controls. Devices must be locked when unattended and protected from unauthorised access or viewing.

Remote access should use approved Trust services. Public or insecure networks should be avoided where possible or used with appropriate caution.

Lost or stolen devices must be reported immediately so that access can be removed or restricted and protective action taken.

16. Social Media

Users must maintain clear professional boundaries online, identify themselves appropriately, and avoid bringing the Trust into disrepute. Confidential information, student information and internal matters must not be shared inappropriately on social media or public platforms.

Personal views must not be presented as Trust views unless the user is authorised to speak on the Trust's behalf.

Staff must not speak on behalf of the Trust in forums, online communities or public discussion platforms unless they are formally authorised to do so.

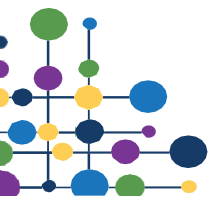
Contact with students through personal social media must not take place unless there is a clear, approved and lawful reason.

17. Personal Devices (BYOD)

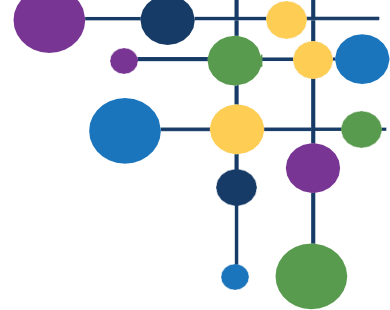
Personal devices may be allowed to access Trust systems under controlled conditions. Devices must meet minimum security requirements, including encryption, software updates, screen lock and appropriate user controls.

Personal devices must not be used to store sensitive Trust information locally unless this has been explicitly authorised and protected appropriately.

The Trust may restrict or remove access from personal devices where a risk is identified. The Trust is not responsible for loss of or damage to personal devices.



Connecting a personal device to the Trust network is at the user's own risk. The Trust is not liable for any hardware or software loss, damage, malfunction or inconvenience arising directly or indirectly from connection to its Wi-Fi services. Users are responsible for ensuring that any software installed on their personal device is properly licensed.



18. Trust Wi-Fi and Network Access

Where Trust Wi-Fi is provided, its use will be monitored and managed proportionately to support safeguarding, security and network performance.

Support for personal devices using Trust Wi-Fi is limited, and the Trust is not responsible for faults or issues affecting those devices.

Trust Wi-Fi must be used appropriately. Users must not bypass security controls, connect unauthorised devices or infrastructure, use staff credentials to connect student devices, or use the service for prohibited activity. Unmanaged IoT devices, hotspots, smart speakers and similar equipment must not be connected to the Trust network.

Students are not permitted to connect personal devices to the Trust Wi-Fi, an exception to this is the sixth form college students.

Guest Wi-Fi is provided for internet access only and must be requested by a Trust staff member. The network is segregated, throttled and subject to Trust security and monitoring requirements.

Guests and sixth form students should not expect privacy and must use the service only for Trust school activities.

Guest and sixth form student devices connected to Trust Wi-Fi are not supported by IT services and are used at the owner's own risk. Access may be withdrawn at any time.

19. Incident and Breach Management

All cyber incidents, data breaches, system outages, lost devices, suspected phishing attacks and other significant ICT issues must be reported immediately through the approved escalation route.

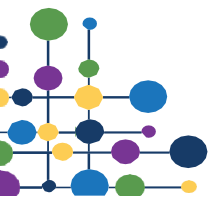
Incidents will be managed in a structured way by identifying, containing, investigating, resolving and reviewing them. Safeguarding concerns will be escalated in line with Trust safeguarding procedures, and data incidents in line with Trust data protection arrangements.

Serious misuse or breaches may result in disciplinary action, restricted access, referral to external agencies or legal action where appropriate.

20. Training and Awareness

The Trust will maintain a cyber security awareness plan for staff and students. This will include induction training, regular awareness activities, targeted guidance on emerging threats such as phishing and cyber-attacks, and updates following significant incidents or technology changes.

The Trust will help staff understand the risks and benefits of new technologies and promote a culture of safe digital practice.



21. Monitoring and Compliance

The Trust will carry out reasonable and proportionate monitoring of systems and activity to protect people, data and services, and to support investigations, safeguarding and compliance.

Compliance checks, audits and reviews will be used to confirm that systems and practices remain aligned with policy, security expectations and statutory requirements.

The Trust will monitor implementation of its cyber security and awareness arrangements and review their effectiveness periodically to ensure they remain aligned with DfE standards and evolving cyber risks.

22. Continual Improvement

The Trust will review ICT services, incidents, risks, user feedback and assurance activity to identify opportunities to improve service quality, resilience, compliance and user experience.

Where improvements are agreed, actions will be planned through the Trust's five-year school action and budget plan, then implemented and reviewed to confirm they achieve the intended outcomes.

23. Photographs and Photography

Photography in schools must comply with the UK GDPR, the Data Protection Act 2018 and the Human Rights Act 1998. These requirements protect personal information and privacy. Restrictions on photography also arise from safeguarding and copyright considerations.

Photography includes photographs, streaming media, transparencies, video, film and digital images created using cameras, video cameras, phones, tablets and similar devices.

Staff may photograph students and staff for the following purposes:

- Student administration
- Curriculum or coursework
- EYFS profile record keeping and evidence gathering
- Corporate and community activities

Before taking a photograph, the Trust must obtain consent from the person photographed if they are over 16, or from a parent or carer for younger students.

Staff must follow the commitments set out in the consent form, including:

- Not naming the student
- Not using the photograph out of context
- Not using the photograph to illustrate sensitive or negative issues

When photographing students, staff must:

- Check that parents or carers have given permission through the consent form. Each school will keep a central list of students without media consent, and staff must check this before using any student images.
- Ensure students are appropriately dressed
- Avoid images showing a single child without context of what they are learning or doing. Identification photographs may be kept for several years but must be deleted when replaced or expired.
- Do not use images of students considered vulnerable
- Avoid naming students. If a name is needed, use only the first name
- Use images that reflect the diversity of participating students

- Report concerns about inappropriate or intrusive photography to the Designated Safeguarding Lead
- Do not use images likely to cause distress, upset or embarrassment

Staff should use school equipment wherever possible when recording images of students. Personal equipment may only be used in exceptional circumstances, such as equipment failure or an unexpected event. Any images taken on personal equipment must be transferred to the school at the earliest opportunity and deleted from the staff member's device, including mobile phones.

24. Artificial Intelligence (AI) and Generative AI Usage

The Trust recognises that AI, including generative AI, may support teaching, learning, accessibility, productivity and administration when used responsibly. However, AI also introduces risks relating to accuracy, bias, privacy, safeguarding and academic integrity.

AI use within the Trust must be safe, lawful, transparent and subject to appropriate human oversight. AI should support professional judgement, not replace it.

Users must not enter personal, confidential or safeguarding-sensitive information into AI tools unless the tool has been formally approved for that purpose and the use is lawful, necessary and secure.

AI-generated content must be reviewed and verified before use. Staff remain accountable for the quality, accuracy and appropriateness of material used with students, families or colleagues.

Students should only use AI where it is permitted and supervised appropriately. AI must not be used to cheat, plagiarise or misrepresent authorship.

Only approved AI tools should be used for Trust-related activity. AI tools should be considered for educational value, security, safeguarding, accessibility and data protection before adoption.

The Trust will provide guidance and awareness on responsible AI use and review this section regularly as DfE guidance and technology develop.

25. Schedule of Amendment

Version No.	Date of Issue	Amendment
2.5	March 2024	Updates to section 1, 8 and 10
2.6	27.3.25	Reviewed with no changes
3.0	July 2026	Substantial rewrite



Appendix A – Core Operational Procedures

Incident Management Procedure

All incidents must be logged through the IT helpdesk or approved escalation route. Incidents will be prioritised by impact and urgency, then assigned for action. The IT service will diagnose, contain where needed, resolve and record the actions taken. Tickets will only be closed when the issue is resolved or otherwise concluded in line with process. Recurring incidents will be reviewed to identify whether further preventive action is needed.

Change Management Procedure

Changes to systems or services must be requested through an approved process. Requests must include a clear description, reason, risk, impact and, where needed, a rollback plan. Approvals must be obtained before implementation, with testing completed where appropriate. Major or high-risk changes must be scheduled to minimise disruption and reviewed afterwards.

Account Lifecycle Procedure

Accounts must only be created following an authorised request and appropriate identity checks. Access must be granted by role and updated promptly when responsibilities change. Accounts must be disabled or removed promptly when a user leaves or no longer needs access.

Asset Control Procedure

New devices must be recorded in the asset register before allocation. Users receiving devices must acknowledge responsibility for their secure use and care. Devices must be securely wiped and removed from records when retired or disposed of.

Data Breach Procedure

Any suspected data breach must be reported immediately to the appropriate Trust contacts. The breach must be contained as quickly as possible and assessed for scope, severity and impact. Actions, decisions and outcomes must be documented in line with Trust arrangements.

Backup and Recovery Procedure

Backups must run to the agreed schedule and be monitored for success. Recovery testing must be carried out periodically for important services and data sets. Where recovery is needed, data integrity and service availability must be validated before return to use.

AI Tool Approval Procedure

Any proposed AI tool for Trust use must be reviewed for educational value, safeguarding, accessibility, security and data protection. Approval must state whether the tool is suitable for staff use, student use or both, and set out any restrictions. Guidance must be provided before widespread adoption, including examples of approved and prohibited use.

