Educational Technology Strategy

Document Detail	
Category	Non-statutory
Department	Academies within the Trust
Responsible Officer	Headteacher
Approved by:	Directors Resources, Risk and Audit committee Chief Executive Officer Academy Committee
Status	Approved 14.4.26
Reviewed on:	Term 3 – 2025/26
Next review:	Term 3 – 2027/28

Contents

Education Technology Strategy & Policy

1. Purpose and scope

This Education Technology Strategy and Policy sets out the strategic priorities, expectations, and operational standards governing the use of digital technologies across the Trust's primary academies.

It ensures that: -

- Technology meaningfully improves teaching, learning, leadership, and administration.
- Staff, pupils, and parents understand their responsibilities regarding technology use.
- All digital systems meet legal and statutory requirements including UK GDPR and the Data Protection Act 2018.
- Technology is used safely, responsibly, and consistently across all academies within the Trust.
- Risks are properly managed, including cyber threats, data breaches, and safeguarding concerns.
- Digital resources and equipment are procured, maintained, and disposed of in a compliant, cost-effective and sustainable way.

This policy applies to all staff, pupils, volunteers, governors, contractors, and third-party providers engaged in the use or management of Trust technology systems.

2. Vision for technology in learning

The Trust aims to create a digital environment where technology is purposeful, accessible, secure, and aligned with the Trust's educational goals. Technology should support excellence in teaching, improve operational efficiency, and prepare pupils for the digital world.

Core Principles

Teaching and learning first

Technology must: -

- Enhance curriculum delivery and increase pupil engagement.
- Support adaptive learning, personalised tasks, and timely feedback.
- Enable high-quality teaching regardless of location or circumstance.
- Allow teachers to gather, analyse, and respond to assessment data more efficiently.

Equity and inclusion

The Trust ensures digital opportunities are available to all pupils by: -

- Providing devices or access support where disadvantage exists.
- Ensuring SEND pupils have appropriate assistive technology.
- Making digital content accessible, using alt text, captions, immersive readers, and other inclusive tools.

Sustainability and value for money

The Trust will: -

- Adopt a lifecycle approach to device and software management.
- Prioritise cost-effective, energy-efficient, and interoperable technologies.
- Ensure procurement decisions support long-term growth.

Security and resilience

The Trust commits to: -

- Maintaining strong cybersecurity across all academies.
- Ensuring disaster recovery and continuity plans are in place.
- Using secure, GDPR-compliant platforms for all data and communication

3. Information management

High-quality information governance underpins all Trust digital activity.

The Trust ensures: -

- Compliance with UK GDPR and the Data Protection Act 2018 through policy, training, audit and oversight from the DPO.
- Daily automated backups of critical systems and cloud-based storage solutions for resilience.
- A full Information Asset Register (IAR) and IT Asset Register, reviewed annually.
- Regular audits to identify risks, vulnerabilities, and opportunities for improvement.
- Role-based access control (RBAC) to ensure only authorised staff access sensitive data.
- Data Protection Impact Assessments (DPIAs) for new platforms, apps, cloud systems, or high-risk processing.
- Data retention follows the Trust Records Management Schedule, with secure deletion of expired data.
- Encryption of devices containing personal or sensitive information.
- Secure data-sharing agreements when working with external partners or cloud providers.

4. Roles and responsibilities

Role	Education Technology Strategy and Policy Responsibilities
Board of Directors	• Approves this strategy and receives assurance of compliance • Ensures appropriate funding for infrastructure and cyber resilience
Trust Central Team	• Delivers and monitors the implementation of the strategy • Maintains asset registers • Oversees Trust-wide consistency and support
IT Manager	• Ensures network stability, security, filtering, and monitoring • Manages user accounts, device deployment, patching, antivirus, endpoint protection • Leads cyber incident response • Advises schools on procurement & digital improvement
Data Protection Officer (DPO)	• Monitors compliance with GDPR • Reviews DPIAs and data breaches • Provides training and advice
Headteachers	• Implement policy at school level • Ensure staff follow digital safeguarding expectations • Oversee filtering/monitoring reports and escalate concerns
All Staff	• Use technology professionally and responsibly • Report incidents promptly • Follow AUP and safeguarding policies • Maintain data accuracy and confidentiality
Pupils & Parents	• Follow digital expectations • Use systems safely and appropriately • Report concerns to staff

5. Copyright and licensing

The Trust ensures that: -

- All digital resources respect copyright and licensing laws.
- Staff only use licensed images, videos, and teaching materials.
- Software and apps are installed only following IT Manager approval.
- No unauthorised copying, downloading, or sharing of copyrighted materials occurs.
- Staff understand Creative Commons licensing and fair-use expectations.

6. Safe communication

To ensure safe and professional communication: -

- Staff must use Trust email and approved communication systems only.
- Personal accounts or messaging apps (WhatsApp, Facebook Messenger etc.) must not be used for pupil interactions.
- Pupils communicate only via supervised, Trust-approved platforms.

- All digital communication must be professional, factual and safeguarding-compliant.
- Communication records must be retained as required.
- Video conferencing for pupils must follow established protocols: -
  - Neutral/blurred backgrounds
  - Approved platforms only
  - No unsupervised 1:1 sessions
  - Recording only with explicit permission

7. Online technologies & safety

The Trust ensures: -

- Filtering and monitoring systems meet DfE statutory standards and cover all devices.
- Monitoring alerts are reviewed daily and escalated appropriately.
- Official social media accounts only are used for school communication.
- Online safety education is embedded across the curriculum (EYFS–KS2).
- Staff complete annual safeguarding & cybersecurity training.
- Pupils receive age-appropriate lessons on:
  - Online behaviour
  - Misinformation
  - Cyberbullying
  - Digital footprints
  - Safe searching

8. Digital systems used

Learning Tools	• Microsoft Teams • Tapestry • ClassDojo • Online curriculum platforms (where approved)
Admin Systems	• Pupil Asset • STAR • Risk Manager • Email, HR and finance systems
Safeguarding Systems	• CPOMS
Security Systems	• Endpoint protection • Firewalls • Filtering & Monitoring software • Multi-Factor Authentication (where possible)

All systems must undergo DPIA review and approval before adoption.

9. IT procurement & maintenance

Procurement is carried out in line with Trust financial regulations and includes: -

- Purchase of Trust-approved devices meeting minimum specification.
- Ensuring warranties and support packages are in place.
- Maintaining an accurate and up-to-date asset register.

Maintenance includes: -

- Regular security and system updates.
- Routine health checks on networks and devices.
- Scheduled replacements based on a 3–5 year lifecycle.
- Patch management for all devices and servers.

10. Disposal of Redundant IT Equipment

Disposal must follow: -

- Secure data wiping using certified erasure tools.
- WEEE-compliant recycling by approved providers.
- Asset register updates identifying withdrawn and destroyed equipment.
- Retention of certificates of destruction for audit.

11. Policy compliance

- Breaches of this policy may lead to disciplinary action.
- All digital incidents (data breaches, cyber events, safeguarding alerts) must be reported immediately to:
  - Headteacher
  - IT Manager
  - DPO
- Non-compliance is monitored through audits, training records, and incident logs.

12. Risk Management & Compliance

To ensure robust digital governance: -

- Annual EdTech risk assessments are completed for each academy.
- Incidents must be reported within 24 hours.
- Staff must undertake cyber incident simulations and scenario-based training.
- Vulnerability scans or penetration testing may be commissioned if required.
- Risks and mitigations are logged in the Trust's central risk register.

13. Review

This policy is reviewed annually or earlier if: -

- National guidance (DfE, NCSC, ICO) changes.
- New technologies introduce additional risk.
- A safeguarding or cyber incident prompts a policy amendment.

Appendix A: Glossary of Terms

Acceptable Use Policy (AUP)	Rules for safe and responsible use of Trust technology systems.
Adaptive Learning	Digital tools that adjust content based on learner performance
Asset Register	Record of all Trust-owned digital equipment
Assistive Technology	Devices or software supporting SEND pupils, e.g., screen readers
Backup	Secure copy of data for restoration after incidents
BYOD (Bring Your Own Device)	Use of personal devices for school purposes (if permitted)
Cloud Storage	Online storage accessible via the internet (e.g., Microsoft 365).
Cybersecurity	Protection of digital systems against attacks and unauthorised access
Data Breach	Incident where personal data is lost or accessed unlawfully
DPIA	Assessment of risks when processing personal data
Endpoint Protection	Security tools such as antivirus and firewalls on devices
Filtering and Monitoring	Systems blocking harmful content and monitoring online behaviour
GDPR	UK law governing protection and processing of personal data
Incident Response Plan	Steps to follow during a cyber or data incident
Infrastructure	Underlying hardware and networks that power digital systems
Learning Platform	Digital environments for teaching (e.g., Teams, Google Classroom).
MFA	Security requiring more than one verification step
MIS	Management Information System storing pupil and school data
Online Safety	Teaching and measures to protect users online
Patch Management	Applying updates to fix vulnerabilities
Personal Data	Information identifying an individual
RBAC	Controls granting system access based on job role
Safeguarding Platform	Systems like CPOMS for recording safeguarding concerns
SSO	Single Sign-On allowing access to multiple systems with one login
WEEE	Regulations for safe disposal and recycling of IT equipment