INFORMATION TECHNOLOGY (IT) POLICY

Approved By: Trust Board
Approval Date: July 2025

CONTENTS

1. PURPOSE

The Girls' Learning Trust ("the Trust") is committed to using technology effectively, securely, and responsibly to support high-quality education and operational efficiency across all its schools. This policy sets out how IT systems, infrastructure, and digital services are managed to enable safe, reliable, and inclusive access for all users.

The policy is designed to:

- Ensure compliance with relevant legal, regulatory, and cybersecurity standards across all Trust schools.
- Align with the Trust's mission and values by promoting digital inclusion, safeguarding, and sustainability.
- Guide schools in the effective use of IT resources to enhance teaching, learning, and administration.
- Define roles, responsibilities, and expectations for staff, students, and other users of Trust IT systems.
- Provide specific additional advice and guidance for the effective and safe use of artificial intelligence.

2. SCOPE

This policy applies to all schools within the Girls' Learning Trust and covers all users of Trust-owned or Trust-managed IT systems, including staff, students, governors, and third-party providers. It applies to both on-site and remote use of devices, software, services, and data under the control of the Trust.

3. DEFINITIONS

Information Technology (IT)
Information Technology refers to the systems, software, networks, and digital tools used to store, process, and communicate information across the Trust. This includes internet access, internal networks, cloud services, learning platforms, and both fixed and mobile devices.

Users
Users are all individuals who access or interact with Trust IT systems. This includes students, staff, governors, contractors, and authorised visitors with temporary or restricted access to devices or systems.

IT Assets
IT assets include any hardware, software, or digital service owned, leased, or managed by the Trust. This covers laptops, desktops, servers, mobile devices, licensed software, and online platforms such as email, storage, or virtual learning environments.

Cybersecurity
Cybersecurity refers to the protection of systems, networks, and data from digital threats such as malware, phishing, and unauthorised access. It includes both technical measures and user behaviours that keep information safe and systems secure.

Data Breach
A data breach is any incident where personal, sensitive, or confidential data is lost, accessed, altered, or shared without permission. This may result from human error, cyberattack, or misuse of systems or devices.

Acceptable Use

Acceptable Use refers to the safe, responsible, and legal use of IT resources in line with Trust policies. All users are required to follow Acceptable Use Agreements, which set out expected conduct and prohibited behaviours.

Remote Access
Remote access allows users to securely connect to Trust systems or data from outside school premises. This includes the use of cloud services, virtual desktops, and secure login tools approved by the Trust.

Cloud Computing
Cloud computing refers to the use of internet-based platforms to store, manage, and process data instead of relying on local servers or devices. Examples include Microsoft 365, Google Workspace, and other cloud-hosted systems used for collaboration and file storage.

Bring Your Own Device (BYOD)
BYOD refers to the use of personal devices—such as smartphones, tablets, or laptops—for work or learning within the Trust. Any personal device used for Trust purposes must comply with security standards and may be subject to monitoring or access restrictions.

Generative Artificial Intelligence
Generative artificial intelligence ("artificial intelligence") is defined as a form of AI that utilises machine learning models to perform tasks including (but not limited to) the creation of new content, such as images, text, video, code or audio based on patterns and structures learned from large amounts of existing data, and in response to user provided prompts.

4. LEGISLATION AND GUIDANCE

This policy is informed by the following legislation and regulatory guidance:

- Data Protection Act 2018 and UK GDPR
- Computer Misuse Act 1990
- Education Act 1996
- Freedom of Information Act 2000
- Keeping Children Safe in Education (KCSIE)
- DfE Meeting digital and technology standards in schools and colleges (2025)
- DfE Cyber Security Standards for Schools and Colleges (2023)
- National Cyber Security Centre (NCSC) guidance
- JCQ's AI Use in Assessments guidance

This policy should be read alongside other relevant Trust and school policies, including:

- Critical Incident Policy and Procedure
- Data Protection and FOI Policy
- Records Retention Policy
- CCTV Policy
- Safeguarding and Child Protection Policy
- Staff Code of Conduct and other HR policies
- Risk Management Policy

5. ROLES AND RESPONSIBILITIES

Trust Board

The Board holds strategic accountability for ensuring that IT provision supports the Trust's aims and complies with legal and regulatory requirements. It approves this policy and monitors risk, data protection, and IT security through oversight reports and assurance mechanisms.

Chief Executive Officer (CEO)
The CEO provides overall leadership and direction for IT strategy across the Trust. This includes ensuring adequate investment in digital infrastructure, managing cyber risk at the executive level, and promoting digital maturity across schools.

Chief Infrastructure Officer (CIO)
The CIO is the "Digital Lead" as per the DfE standards and is responsible for operational delivery of IT systems and services. This includes oversight of procurement, IT service delivery, compliance, and incident response, working closely with Trust IT staff and external providers.

Head of IT
The Head of IT provides technical leadership across the Trust, ensuring IT systems are secure, reliable, and aligned with Trust policy and national standards. Working closely with the Chief Infrastructure Officer and school-based IT staff, they lead on cybersecurity, access management, infrastructure oversight, and incident response. They coordinate the work of IT Leads and Network Managers, ensure compliance with data protection and DfE digital standards, and manage supplier relationships to maintain effective service delivery.

Headteachers
Headteachers ensure that IT systems in their schools support educational goals and are used in a safe, effective, and inclusive manner. They oversee implementation of this policy, ensure staff compliance, and support digital safeguarding and CPD.

Head of IT / IT Leads / Network Managers
These staff manage the technical operation of IT infrastructure within schools. They are responsible for security, maintenance, user access, troubleshooting, and ensuring systems function effectively in line with policy and guidance.

Teaching and Support Staff
All staff are responsible for the appropriate use of Trust IT systems, safeguarding student data, and following security protocols. They are expected to model safe and responsible digital behaviour and report any concerns or breaches promptly.

Students
Students must use school IT systems responsibly and in line with the school's acceptable use agreements. They are expected to protect their login credentials, respect digital boundaries, and seek help if they encounter online risks or issues.

Parents and Carers
Parents are expected to support their children in using school technology appropriately and safely, particularly in home learning contexts. Schools will keep parents informed about online safety, IT expectations, and digital tools in use.

6. UNDERPINNING PRINCIPLES

The Trust's approach to IT is built on six core principles that support inclusion, security, sustainability, and improvement across all schools.

Inclusion and Accessibility

All users must have fair and supported access to IT systems, ensuring that no student or staff member is disadvantaged by digital barriers. Systems should be designed or selected to meet a wide range of accessibility needs.

- Schools must provide appropriate devices, access, or adjustments to meet individual needs.
- Digital exclusion should be addressed through targeted support and equitable resource allocation.

Security and Safeguarding

Protecting users and data is central to the Trust's use of technology. Systems must be secure and resilient, and online risks actively managed in line with safeguarding responsibilities.

- Cybersecurity controls (e.g. filtering, encryption, access controls) must be maintained and regularly reviewed.
- All staff and students must be trained to recognise and report online risks or incidents.

Sustainability and Value

IT decisions should offer long-term value and reflect environmental responsibility. The Trust seeks to use digital resources efficiently while minimising waste and energy use.

- Devices and infrastructure should be chosen for quality, lifespan, and ease of maintenance.
- Obsolete equipment must be recycled responsibly in line with data disposal standards.

Innovation and Continuous Improvement

Technology should be used to enhance learning and efficiency, not as an end in itself. The Trust encourages responsible innovation that improves outcomes and supports staff development.

- Schools are supported to trial and adopt effective digital tools aligned with educational goals.
- Staff and students should have opportunities to build their digital skills and confidence.

Consistency and Compliance

All schools must follow Trust-wide IT standards and policies to ensure consistency, security, and legal compliance. Local adaptations must not compromise data protection or cyber safety.

- Approved systems, platforms, and vendors should be used unless agreed otherwise.
- Any new IT tools must be assessed for risk and authorised before use.

Accountability and User Responsibility

All users are expected to act responsibly, ethically, and in line with Trust expectations. Misuse of IT systems may lead to disciplinary action or safeguarding referrals.

- Acceptable Use Agreements must be in place and communicated to all users.
- Concerns about misuse or breaches must be reported and acted upon without delay.

7. SAFEGUARDING

The Trust is committed to ensuring that all digital activity across our schools supports, rather than compromises, the safety and wellbeing of students and staff. Safeguarding is a core responsibility of all users of Trust IT systems and applies equally in online and offline contexts.

All IT use must comply with the Trust's Safeguarding and Child Protection Policy, which sets out our overarching commitment to child welfare, the role of designated safeguarding leads (DSLs), and

expectations for digital safety. Particular care must be taken when using, sharing, or storing personal or sensitive information, engaging with students online, or using communication tools within or beyond the classroom.

Staff must be alert to safeguarding risks linked to digital technologies, including:

- Online bullying, grooming, radicalisation, or exposure to harmful content.
- Inappropriate sharing of images, messages, or personal data.
- The use of unmonitored platforms, personal devices, or unsupervised communications.

Designated Safeguarding Leads work closely with IT teams to oversee filtering, monitoring, and digital safeguarding strategies. Where users have concerns about a child's safety in a digital context, they must follow the same procedures as for any other safeguarding concern.

8. ACCEPTABLE USE

All users of the Trust's IT systems—staff, students, governors, and authorised visitors—are expected to use technology safely, respectfully, and in line with the Trust's policies. Acceptable use applies to any device or service connected to the Trust network, including personally owned devices where permitted. By accessing Trust systems or networks, users agree to the following:

- Use only your assigned login credentials and keep passwords secure and confidential.
- Ensure that all activity—whether on school devices or personal devices using Trust systems—is appropriate, lawful, and related to professional duties or educational purposes.

Users must not:

- Access, create, or share material that is offensive, illegal, discriminatory, or harmful.
- Introduce security risks, such as installing unauthorised software, bypassing filtering systems, or attempting to access restricted areas of the network.

Email and internet use should follow the same standards expected in any professional or educational communication. Language must be respectful, and users are responsible for the content they send, access, or forward.

The Trust may monitor the use of its systems, including emails, web activity, and file storage, to ensure compliance with this policy and fulfil its legal and safeguarding duties. Inappropriate use may result in disciplinary action or withdrawal of access.

All users are expected to:

- Respect the privacy and data of others, and follow data protection principles at all times.
- Report concerns, accidental breaches, or suspicious activity to the Trust's IT team or senior leadership immediately.

9. SYSTEMS AND CYBER SECURITY

<u>Core Cyber Security Principles</u>
The Trust implements a risk-based, whole-system approach to cyber security. Systems must be:

- Proportionate: safeguards must reflect the size, complexity, and risk profile of the Trust and each school.
- Multi-layered: controls should be technical (e.g. antivirus), behavioural (e.g. staff awareness), and

procedural (e.g. response plans).
- Regularly reviewed: risk assessments and security audits must be undertaken at least annually and reviewed termly.
- Linked to continuity planning: all schools must include cyber security in their critical incident policy and procedure.

Equipment and Physical Security

All Trust-owned devices—such as laptops, tablets, and desktop computers—must be secured against loss, theft, or damage. Users are responsible for the physical care and appropriate use of equipment assigned to them.

- Devices must be locked, logged off, or shut down when unattended.
- Staff must never leave equipment in unsecured areas, especially vehicles.
- ICT hardware must not be moved, altered, or tampered with without approval from the IT team.
- Screens handling sensitive data should not be visible to unauthorised individuals, especially in public or shared spaces.
- Equipment used off-site must be treated with the same level of care as if used on Trust premises.

Passwords and Account Management

User credentials form the front line of cyber security. All users must have unique login details and follow secure password practices.

- Passwords should be strong, confidential, and follow the recommended format of three random words.
- Sharing passwords or leaving systems logged in for others to access is strictly prohibited.
- Access to Trust systems must be via authorised accounts only, and account privileges should reflect the minimum level required for a user's role.
- Access rights must be reviewed regularly and removed promptly when a user leaves or changes role.

Multi-factor authentication should be enabled wherever supported, especially for systems accessing sensitive data.

Software, Applications and Updates

Only authorised software and apps may be installed or used on Trust systems. Unauthorised installations pose a risk to network integrity and data protection.

- Software must be sourced through official channels and checked by IT support before installation.
- Automatic updates should be enabled where possible to ensure software remains supported and secure.
- Users must not disable antivirus programs, firewalls, or endpoint protection tools.

Any request to install third-party or specialist software must be reviewed for security risk, licensing compliance, and compatibility with the Trust's IT environment.

Network, Filtering and Monitoring

The Trust uses filtering and monitoring tools to protect users, safeguard students, and block access to inappropriate or malicious content.

- Schools must implement age-appropriate web filtering that meets DfE standards.
- Monitoring systems may include logging of web activity, keyword detection, and email scanning.
- Attempts to bypass filters or access unauthorised areas of the network are a breach of this policy.
- The Trust reserves the right to inspect network activity and device use as part of its safeguarding

and compliance obligations.

Network configuration, including cabling, IP settings, and server access, must be managed exclusively by authorised IT staff or contractors.

Remote Access and Cloud Platforms

The Trust enables remote access through secure, approved channels only. Whether working from home or using cloud platforms like Microsoft 365 or Google Workspace, users must follow robust security protocols.

- Remote access should use secure connections (e.g. VPNs, MFA-protected logins) to reduce risk.
- Staff must avoid working with confidential material in public or unsecure settings (e.g. trains, cafés).
- Files stored in the cloud must be shared appropriately and access-controlled based on user role.
- Sensitive documents should not be downloaded to personal or shared devices unless encrypted and strictly necessary.

Schools must ensure that any cloud services comply with UK GDPR and have clear data processing agreements in place.

Data Handling, Loss and Disposal

Users must take care when storing, transferring, or deleting data to avoid breaches and comply with data protection law.

- Sensitive or personal data must be encrypted or password protected if stored on portable or personal devices.
- Lost or stolen equipment must be reported to the IT team immediately, regardless of whether it is school- or personally owned.
- Any equipment being decommissioned or transferred must be wiped securely before disposal or reallocation.
- Trust systems must not be used to store personal files, photos, or unrelated data.

Staff should use approved platforms for managing and storing confidential data.

Incident Response and Reporting

The Trust maintains a clear procedure for detecting, reporting, and responding to cyber incidents and data breaches. All users must:

- Report suspected security breaches, phishing attempts, or device loss to the IT team or school lead immediately.
- Avoid taking remedial action (e.g. deleting suspicious files) without consulting IT support.
- Cooperate fully with investigations following a breach or incident.
- Understand that incidents may be escalated to the DPO, external authorities, and/or insurers depending on severity.

The Trust's Cyber Response Plan forms part of the wider Critical Incident Policy and Procedure planning framework. It is tested annually and updated in response to new threats or lessons learned.

10. BRING YOUR OWN DEVICE (BYOD)

The Trust recognises that staff and students may wish to use their own devices to access Trust systems and services. Where Bring Your Own Device (BYOD) is permitted, it must be managed carefully to protect data security, comply with legal obligations, and maintain system integrity. Use of personal

devices for Trust-related purposes is a privilege, not an entitlement. It must be authorised in advance and is subject to the following expectations:

Device Security and Compliance

- Personal devices must be protected by a secure password or biometric authentication and have an automatic screen lock enabled.
- All devices used for Trust work must be kept up to date with the latest security patches, operating system updates, and reputable antivirus software.
- Devices must not be "jailbroken" or rooted, as this removes manufacturer protections and introduces risk.

Access and Usage

- Access to Trust systems (e.g. email, cloud platforms, remote desktop) must only be through secure and approved channels, such as multi-factor authentication or managed apps.
- Users must not attempt to access restricted systems, share login details, or install Trust-owned software on personal devices without authorisation.
- The Trust may restrict BYOD use to certain roles, activities, or platforms and reserves the right to withdraw access at any time.

Data Storage and Protection

- Trust data must never be stored unprotected on a personal device or removable media such as USB sticks.
- Documents and records containing personal, sensitive, or confidential data must only be accessed through secure cloud services and not downloaded locally unless essential and encrypted.
- Users must not sync personal devices with Trust accounts in a way that duplicates or caches data onto unsecured applications (e.g. unapproved mail clients or cloud backup services).

Loss, Theft or Transfer

- Any personal device used for Trust purposes that is lost, stolen, infected, or compromised must be reported to the IT team immediately.
- Where a device contains Trust data, appropriate steps must be taken to remotely wipe or secure that data.
- Personal devices must be wiped of all Trust data before being sold, passed to another user, or disposed of.

Responsibilities and Monitoring

- Users must read and sign the Trust's BYOD Protocol before connecting a personal device to Trust systems.
- BYOD use is subject to monitoring in line with the Trust's Acceptable Use and Data Protection policies. While personal content is not routinely accessed, activity on Trust systems may be logged for security purposes.
- The Trust accepts no responsibility for damage to, or loss of, personal devices used for work purposes, except where such damage results from the negligence of the Trust or its staff.

11. ARTIFICIAL INTELLIGENCE

The Trust acknowledges the increasing presence and potential of Artificial Intelligence (AI) technologies in education, administration, and operations. AI, when used appropriately, can support innovation, enhance productivity, personalise learning, and streamline processes. However, it also brings risks—particularly around bias, data privacy, accountability, and misuse—that require clear governance and responsible implementation.

Please see the AI Policy for more information.