ACT MULTI ACADEMY TRUST

ACCEPTABLE USE POLICY

ICT, DIGITAL SYSTEMS, EMAIL, INTERNET, DEVICES, ONLINE SAFETY, AI AND COMMUNICATIONS

(Operates in accordance with the Trust's Cyber Security, Data Protection, Safeguarding, Online Safety, AI, Records Management, Disciplinary and Business Continuity frameworks)

Document Control

Item	Detail
Policy Name	Acceptable Use Policy
Version	Draft V1.0
Author	Chief Executive Officer / Chief Financial Officer / Data Protection Officer
Applicable To	All employees, trustees, governors, volunteers, contractors, consultants, agency staff, visitors and any other authorised users of Trust systems
Approved By	Trust Board
Committee Oversight	Finance, Audit and Risk Committee / Standards and Education Committee where safeguarding and online safety matters arise
Policy Owner	Chief Financial Officer
Operational Leads	Chief Financial Officer, Data Protection Officer, Director of Inclusion/Safeguarding, Director of Education, IT Support Partner, Headteachers
Approval Date	July 2026
Effective From	Immediate upon approval
Review Cycle	Annual, or sooner in response to legislative, regulatory, safeguarding, cyber security, operational or technological change
Next Review Date	July 2027
Publication	Staff portal / policy portal / Trust intranet / school-level policy folders as appropriate
Related Policies	Data Protection Policy; Cyber Security Policy; Safeguarding and Child Protection Policy; Staff Code of Conduct; Disciplinary Policy; Whistleblowing Policy; Online Safety / Filtering and

Item	Detail
	Monitoring Policy; AI Policy; Records Management and Retention Policy; Freedom of Information Policy; Business Continuity Plan; Finance Regulations

Version Control

Version	Date	Summary of Changes	Approved By
V1.0	July 2026	New Trust-wide Acceptable Use Policy covering ICT systems, email, monitoring, mailbox access, AI, personal devices, cyber security, safeguarding, data protection and business continuity	Trust Board

1. Statement of Intent

ACT Multi Academy Trust is committed to ensuring that all digital systems, devices, email accounts, internet services, applications, cloud services, communication platforms and information assets are used safely, lawfully, responsibly and professionally.

The Trust recognises that digital technology is central to the effective operation of schools, the delivery of education, communication with families, management of finance and HR, safeguarding, governance, compliance and business continuity. The Trust also recognises that inappropriate or insecure use of digital systems can create significant risks, including safeguarding harm, data breaches, cyber incidents, fraud, reputational damage, operational disruption and financial loss.

This policy sets clear expectations for all users. It is intended to protect pupils, staff, trustees, governors, families, Trust assets, confidential information and the reputation of ACT Multi Academy Trust and its schools.

All users are expected to act with integrity, professionalism and due care when using Trust systems or when handling Trust information.

2. Purpose of this Policy

The purpose of this policy is to:

- establish clear standards for the acceptable use of Trust ICT systems, devices, accounts, networks and digital services;
- protect pupils and staff from online and digital risks;
- safeguard Trust data, records, finances and operational information;
- support compliance with UK GDPR, the Data Protection Act 2018, safeguarding legislation and education-sector guidance;
- reduce the risk of cyber incidents, unauthorised access, data loss, fraud and misuse;
- clarify that Trust systems, accounts and records are business resources belonging to the Trust;
- explain the circumstances in which the Trust may monitor, access, retrieve, preserve or review information held in Trust systems;
- support business continuity during absence, suspension, resignation, investigation, emergency or critical operational need;
- provide a clear basis for management action or disciplinary action where this policy is breached.

3. Scope

This policy applies to all users who access or use Trust systems, devices, networks, information or communication platforms, including:

- employees;
- senior leaders;
- headteachers and heads of school;
- trustees and governors;
- volunteers;
- supply staff;
- agency workers;

- consultants;
- contractors;
- trainees;
- visitors;
- third-party service providers;
- any other person given access to Trust systems, devices, platforms or information.

This policy applies whether access takes place:

- on Trust or school premises;
- at home;
- remotely;
- during school trips or off-site activities;
- using Trust-owned equipment;
- using personally owned equipment for Trust business;
- through cloud-based systems;
- through mobile phones, tablets, laptops or other portable devices;
- during or outside normal working hours where Trust systems, accounts or information are being used.

---

4. Key Principles

All users must comply with the following principles:

1. **Trust systems are for Trust business**
   Trust systems, accounts, devices and platforms are provided to support education, safeguarding, governance, administration and the operation of the Trust.
2. **Trust information must be protected**
   Personal, confidential, financial, safeguarding, HR and operational information must be accessed, stored, used and shared only where there is a legitimate Trust purpose.
3. **Safeguarding is paramount**
   Online safety, filtering, monitoring and the safe use of technology are part of the Trust's safeguarding responsibilities.
4. **Cyber security is everyone's responsibility**
   Users must act in ways that reduce the risk of data breaches, phishing, ransomware, malware, unauthorised access and system compromise.
5. **Professional conduct applies online and offline**
   The same standards of professional behaviour apply to digital communications as to face-to-face interactions.
6. **Trust accounts and systems may be monitored or accessed**
   Users must understand that Trust systems, devices, accounts and records may be accessed, monitored, retrieved, reviewed or preserved where the Trust has a legitimate reason and where this is lawful, necessary and proportionate.
7. **Personal use must be limited and appropriate**
   Any personal use of Trust systems must be reasonable, lawful, proportionate, not excessive and not interfere with duties, safeguarding, confidentiality, security or Trust reputation.
8. **Misuse may lead to disciplinary action**
   Breaches of this policy may result in management action, withdrawal of access, disciplinary action, dismissal, referral to external agencies or legal action.

---

5. Definitions

Term	Meaning
Trust systems	Any ICT system, software, platform, network, email account, communication tool, MIS, finance system, HR/payroll system, cloud storage, safeguarding system, device or digital service owned, licensed, managed or used by ACT Multi Academy Trust
Trust information	Any information created, received, stored, accessed or processed for Trust purposes, including pupil, staff, financial, governance, safeguarding, HR, operational, contractual and confidential information

Term	Meaning
User	Any person authorised to access Trust systems, equipment, accounts or information
Monitoring	Reviewing, checking, recording or analysing use of systems, accounts, devices, internet activity, security logs, email traffic, data access, system activity or communications
Business access	Accessing or retrieving information held within Trust systems or accounts for legitimate operational, legal, safeguarding, HR, compliance, audit, financial, investigatory or business continuity purposes
Personal data	Information relating to an identified or identifiable living person
Special category data	More sensitive personal data, including health information, ethnicity, religion, biometric data and other categories defined in data protection legislation
Safeguarding information	Any information relating to the safety, welfare, protection or vulnerability of a child or adult at risk
AI tools	Artificial intelligence and generative AI tools, including but not limited to Microsoft Copilot, ChatGPT, Gemini, Claude, image-generation tools, transcription tools, automated marking tools, adaptive learning platforms and similar services

6. Ownership of Systems, Accounts, Devices and Records

All Trust ICT equipment, email accounts, communication platforms, cloud storage, software licences, data, documents, records and digital systems are the property of ACT Multi Academy Trust or are licensed for use by the Trust.

This includes, but is not limited to:

- Trust-issued laptops, desktops, tablets and mobile phones;
- Trust email accounts;
- Microsoft 365 accounts and associated storage;
- SharePoint, OneDrive, Teams and other collaboration platforms;
- finance systems;
- HR and payroll systems;
- management information systems;
- safeguarding and attendance systems;
- cloud-based files and records;
- Trust-owned documents, spreadsheets, presentations and databases;
- communications created, sent, received or stored for Trust business purposes.

Users must not treat Trust accounts, devices or systems as private personal spaces. Information created, sent, received or stored using Trust systems may constitute a Trust record.

7. No Expectation of Absolute Privacy

Users should have no expectation of absolute privacy when using Trust systems, devices, email accounts, internet services, communication platforms or cloud storage.

The Trust respects the privacy and data protection rights of staff and other users. However, the Trust may access, monitor, retrieve, preserve or review information held within Trust systems where there is a legitimate reason and where doing so is lawful, necessary and proportionate.

Examples of legitimate reasons may include:

- safeguarding concerns;
- child protection investigations;
- allegations involving staff;
- business continuity;
- employee absence;
- suspension;
- resignation or departure;
- suspected misconduct;
- suspected fraud;
- financial control;
- audit and internal scrutiny;

- cyber security;
- data protection compliance;
- subject access requests;
- freedom of information requests;
- legal claims or disputes;
- regulatory obligations;
- operational emergencies;
- recovery of Trust documents, emails or records;
- protection of pupils, staff, assets or public funds.

Any access or monitoring must be undertaken in accordance with this policy, data protection legislation, Trust procedures and relevant authorisation arrangements.

---

8. Roles and Responsibilities

8.1 Trust Board

The Trust Board is responsible for:

- approving this policy;
- ensuring appropriate governance oversight of digital risk, cyber security, data protection, safeguarding and business continuity;
- holding executive leaders to account for implementation;
- ensuring that risks arising from ICT, cyber security, online safety and information governance are considered through the Trust's risk management framework.

8.2 Finance, Audit and Risk Committee

The Finance, Audit and Risk Committee is responsible for:

- overseeing cyber security, data protection, information governance, fraud risk, internal controls and business continuity;
- reviewing assurance reports relating to cyber security, system access, incidents and policy compliance;
- ensuring that digital and information risks are recorded and reviewed through the Trust risk register.

8.3 Standards and Education Committee

The Standards and Education Committee is responsible for:

- oversight of safeguarding and online safety where these relate to pupil welfare, curriculum, teaching and learning;
- receiving assurance that filtering and monitoring arrangements support safeguarding duties;
- ensuring appropriate links between online safety, safeguarding, behaviour, attendance and inclusion.

8.4 Chief Executive Officer

The Chief Executive Officer is responsible for:

- ensuring this policy is implemented across the Trust;
- ensuring that systems, controls, culture and leadership expectations support safe and lawful use of technology;
- authorising high-risk access or monitoring decisions where appropriate;
- ensuring concerns involving senior leaders are escalated appropriately.

8.5 Chief Financial Officer

The Chief Financial Officer is the policy owner and is responsible for:

- oversight of ICT contracts, systems, licences, cyber security, finance systems and operational controls;
- ensuring ICT access arrangements support financial and operational integrity;
- ensuring appropriate controls are in place for access to finance, payroll, procurement and business systems;
- ensuring that mailbox or system access for business continuity is documented and proportionate.

8.6 Data Protection Officer

The Data Protection Officer is responsible for:

- advising on data protection implications of monitoring, access, retrieval and disclosure of information;
- advising on data breaches and reporting requirements;
- supporting data protection impact assessments where required;
- advising on subject access requests, freedom of information requests and information-sharing matters;
- ensuring data protection risks are considered when new systems or technologies are introduced.

8.7 Director of Inclusion / Safeguarding Lead

The Director of Inclusion or Trust Safeguarding Lead is responsible for:

- ensuring that online safety, digital conduct, filtering and monitoring support safeguarding duties;
- advising on digital safeguarding concerns;
- ensuring online safety concerns are escalated and recorded appropriately;
- supporting schools to understand online risk, filtering, monitoring and safeguarding procedures.

8.8 Headteachers and Senior Leaders

Headteachers and senior leaders are responsible for:

- implementing this policy within their school;
- ensuring staff understand expectations;
- ensuring incidents are reported promptly;
- ensuring local procedures are followed;
- ensuring new staff, supply staff, volunteers and relevant contractors are made aware of this policy;
- escalating serious concerns to the Trust central team.

8.9 IT Support Partner

The IT Support Partner is responsible for:

- implementing technical controls as agreed by the Trust;
- maintaining user accounts, access permissions and system security;
- supporting cyber security controls, including multi-factor authentication, password resets, anti-malware and system updates;
- supporting investigation of technical incidents;
- supporting authorised requests for access, retrieval or preservation of Trust records;
- providing technical reports where required for safeguarding, HR, finance, audit, cyber security or data protection purposes.

8.10 All Users

All users are responsible for:

- reading, understanding and complying with this policy;
- using Trust systems lawfully, safely and professionally;
- protecting passwords and access credentials;
- reporting incidents, breaches, concerns or suspected misuse immediately;
- completing required training and acknowledgements;
- following instructions issued by the Trust, school leaders, ICT support and the Data Protection Officer.

---

9. Acceptable Use of Trust Systems

Users may use Trust systems for:

- teaching and learning;
- safeguarding and pupil welfare;
- school administration;
- finance, payroll, HR and operational management;
- governance and trustee business;
- communication with pupils, families, staff, governors, trustees, contractors and external partners;

- professional development;
- approved research and planning;
- authorised remote working;
- any other legitimate Trust purpose.

Users must:

- use systems honestly, responsibly and professionally;
- access only information needed for their role;
- use approved platforms wherever possible;
- keep information accurate and secure;
- comply with data protection, safeguarding and confidentiality requirements;
- respect copyright, licensing and intellectual property rights;
- report concerns immediately.

---

10. Prohibited Use

Users must not use Trust systems, devices, accounts, internet access or platforms to:

- access, create, store, download, upload, transmit or share illegal material;
- access, create, store, download, upload, transmit or share material that is discriminatory, abusive, hateful, violent, extremist, obscene or otherwise inappropriate;
- bully, harass, intimidate or victimise any person;
- impersonate another user;
- access another person's account without authorisation;
- share passwords or authentication codes;
- bypass filtering, monitoring, security controls or access restrictions;
- install unauthorised software, apps, browser extensions or tools;
- introduce malware, ransomware, spyware or viruses;
- access systems or information beyond the user's authority;
- disclose confidential information without authority;
- store Trust information in unapproved personal accounts or consumer cloud services;
- conduct private business, political campaigning or commercial activity;
- engage in excessive personal use;
- bring the Trust or any school into disrepute;
- use systems in a way that creates safeguarding, legal, reputational, operational, cyber security or financial risk.

---

11. User Accounts, Passwords and Authentication

Users must:

- use only their own authorised account;
- keep passwords and authentication details confidential;
- use strong passwords in accordance with Trust requirements;
- use multi-factor authentication where required;
- never share authentication codes or approve unexpected sign-in prompts;
- report suspected account compromise immediately;
- lock screens when leaving devices unattended;
- log out of shared devices after use;
- comply with instructions from ICT support.

Users must not:

- write passwords where others can access them;
- share accounts;
- allow pupils, colleagues, family members or others to use their account;
- use another person's account;
- attempt to access restricted systems;
- ignore suspicious sign-in alerts.

Where a user suspects that their account has been compromised, they must report this immediately to ICT support and their line manager.

---

12. Email and Electronic Communications

Trust email and communication systems are business resources. They must be used professionally, safely and responsibly.

Users must:

- use Trust email accounts for Trust business;
- check recipients carefully before sending;
- use appropriate language and tone;
- consider confidentiality before sending personal or sensitive information;
- use secure methods where required;
- avoid unnecessary distribution of personal data;
- avoid forwarding confidential information to personal accounts;
- report misdirected emails or suspected data breaches immediately;
- use agreed signatures and disclaimers where required;
- retain emails in accordance with Trust retention requirements.

Users must not:

- send offensive, abusive, discriminatory or inappropriate messages;
- use Trust email to harass or intimidate;
- send confidential or sensitive information to unauthorised recipients;
- auto-forward Trust email to personal accounts without authorisation;
- conceal or delete records to avoid disclosure, audit, investigation or regulatory review;
- use personal email accounts for Trust business unless expressly authorised in exceptional circumstances.

Emails created, sent or received through a Trust account may be Trust records and may be accessed, retrieved, reviewed, preserved or disclosed where there is a lawful and legitimate Trust reason.

---

13. Access to Email Accounts and Mailboxes

The Trust may access a Trust email account or mailbox where there is a legitimate operational, safeguarding, legal, regulatory, HR, financial, audit, cyber security or business continuity reason.

Access may be required where a user is:

- absent from work;
- on long-term sickness absence;
- suspended;
- under investigation;
- leaving or has left employment;
- unable or unwilling to retrieve required business information;
- involved in a safeguarding, financial, HR, data protection or governance matter;
- subject to a legal, regulatory, audit or information request;
- holding information needed for urgent operational continuity.

Mailbox access must be:

- authorised by an appropriate senior officer;
- limited to the purpose for which access is required;
- proportionate to the need identified;
- documented;
- undertaken by an appropriate person or ICT support provider;
- conducted in a way that minimises access to personal or irrelevant material;
- subject to advice from the Data Protection Officer where appropriate.

Where possible, targeted searches should be used rather than unrestricted review. Search terms, date ranges, folders, subject matter and access purposes should be recorded where appropriate.

The Trust will not routinely monitor or access mailboxes without reason. However, where a legitimate need exists, Trust email accounts may be accessed without the account holder's prior consent where notification would be inappropriate, impractical, prejudicial to an investigation or inconsistent with safeguarding, legal, regulatory or operational requirements.

---

14. Internet Use

Internet access is provided to support education, safeguarding, communication, administration and Trust operations.

Users must:

- use internet access responsibly;
- comply with filtering and monitoring arrangements;
- report accidental access to inappropriate content immediately;
- avoid unsafe websites and suspicious links;
- avoid downloading files from untrusted sources;
- follow copyright and licensing requirements;
- use professional judgement at all times.

Users must not:

- attempt to bypass filtering or monitoring systems;
- access illegal, harmful, extremist, discriminatory, violent or inappropriate content;
- download unauthorised software;
- use anonymising tools, VPNs or proxy services to avoid Trust controls unless authorised;
- use Trust internet access in a way that creates safeguarding, cyber security, legal or reputational risk.

---

15. Filtering and Monitoring

The Trust will maintain appropriate filtering and monitoring arrangements to support safeguarding, online safety, cyber security and responsible use.

Filtering and monitoring arrangements will seek to:

- prevent access to illegal, inappropriate or harmful content;
- support safeguarding responses;
- identify potential online safety concerns;
- protect systems from malicious or unsafe websites;
- support compliance with statutory and regulatory expectations;
- ensure that pupils and staff can work online safely.

The Trust will review filtering and monitoring provision at least annually and sooner where there are significant changes to systems, risks, providers, safeguarding concerns or statutory guidance.

Staff must be aware that filtering and monitoring systems may generate reports or alerts relating to online activity. Such reports may be reviewed by authorised staff where there is a safeguarding, operational, cyber security or compliance reason.

Users must not attempt to disable, bypass, weaken or interfere with filtering or monitoring arrangements.

---

16. Devices and Equipment

Trust-issued devices remain the property of the Trust.

Users must:

- take reasonable care of devices;
- keep devices secure;
- use devices primarily for Trust purposes;
- install updates when prompted;
- ensure devices are locked when unattended;
- report loss, theft or damage immediately;
- return devices when requested or when leaving employment;
- comply with any device agreement issued by the Trust.

Users must not:

- lend Trust devices to unauthorised people;
- permit family members or others to use Trust devices;
- disable security controls;
- install unauthorised software;
- store excessive personal material on Trust devices;
- use Trust devices for unlawful or inappropriate activity;
- remove asset tags or security settings.

The Trust may inspect, access, wipe, disable or recover Trust devices where necessary for security, maintenance, investigation, business continuity or compliance purposes.

---

17. Personal Devices and Bring Your Own Device

Personal devices must not be used for Trust business unless authorised or permitted under Trust arrangements.

Where personal devices are used for Trust business, users must:

- keep the device secure;
- use password, PIN or biometric protection;
- keep operating systems and apps up to date;
- avoid storing Trust information locally wherever possible;
- use approved Trust systems rather than personal storage;
- ensure other household members cannot access Trust information;
- report loss, theft or compromise immediately;
- delete Trust information when no longer required or when instructed.

Users must not:

- store safeguarding, HR, financial or sensitive personal data on personal devices unless expressly authorised;
- use personal cloud accounts for Trust records;
- take photographs or recordings of pupils on personal devices unless specifically authorised under school procedures;
- allow Trust information to be visible or accessible to others.

The Trust may require Trust information to be removed from personal devices and may restrict access where security requirements are not met.

---

18. Data Protection and Confidentiality

All users must comply with the UK GDPR, Data Protection Act 2018, Trust Data Protection Policy and associated procedures.

Users must:

- access personal data only where needed for their role;
- process personal data lawfully, fairly and transparently;
- keep personal data accurate and secure;
- share information only with authorised recipients;
- use secure methods for sensitive information;
- store information in approved locations;
- avoid unnecessary duplication of personal data;
- follow retention and disposal requirements;
- report suspected data breaches immediately.

Users must take particular care with:

- pupil records;
- safeguarding records;
- child protection information;
- SEND information;
- medical information;
- staff HR records;
- payroll and finance information;
- disciplinary and grievance information;
- trustee and governor records;
- legal advice and privileged material;
- commercially sensitive information.

Confidential information obtained through employment or association with the Trust must not be disclosed without proper authority, during or after employment or engagement.

---

19. Information Classification

Users must apply appropriate care based on the sensitivity of information.

Classification	Examples	Expected Handling
Public	Published policies, website information, public newsletters	May be shared externally if approved and accurate
Internal	Routine operational documents, internal updates, meeting notes not containing sensitive data	Share only within the Trust or with authorised partners
Confidential	HR matters, finance records, governance papers, non-public school improvement information	Share on a need-to-know basis using approved systems
Highly Confidential / Sensitive	Safeguarding records, child protection information, allegations against staff, medical data, disciplinary matters, legal advice, payroll information	Share only with specifically authorised individuals using secure methods and with appropriate recording

Where users are unsure how to classify or share information, they must seek advice before sharing.

---

20. Safeguarding and Online Safety

All users must recognise that online safety is part of safeguarding.
Users must:

- follow the Trust Safeguarding and Child Protection Policy;
- report online safety concerns immediately;
- avoid one-to-one private digital communication with pupils outside authorised systems;
- maintain professional boundaries online;
- report any concern relating to inappropriate contact, grooming, exploitation, bullying, radicalisation, harmful content or pupil welfare;
- follow school procedures for use of images, videos and recordings;
- ensure online platforms used with pupils are approved and risk assessed where appropriate.

Users must not:

- communicate with pupils through personal social media accounts;
- share personal contact details with pupils unless authorised for a specific educational or safeguarding purpose;
- take, store or share images of pupils contrary to consent and school procedures;
- ignore online safeguarding concerns;
- use unapproved platforms for pupil communication.

Any safeguarding concern arising through digital systems, emails, devices, online platforms or social media must be reported in accordance with safeguarding procedures.

---

21. Social Media and Public Communications

Users must maintain professional standards when using social media and digital communication platforms.
Users must not:

- disclose confidential Trust, school, pupil, staff, parent, governance or operational information;
- make comments that could damage the reputation of the Trust or its schools;
- discuss pupils, parents, staff, trustees, governors or sensitive Trust matters inappropriately online;
- post material that is discriminatory, offensive, bullying, harassing or inconsistent with professional standards;
- identify pupils without appropriate permission;
- engage in online disputes on behalf of the Trust unless authorised;
- use the Trust logo, branding or identity without permission.

Personal social media use must not conflict with professional responsibilities, safeguarding expectations or the reputation of the Trust.

---

22. Artificial Intelligence and Automated Tools

The Trust recognises that AI tools can support efficiency, planning, communication and learning when used appropriately. However, AI tools also present risks relating to confidentiality, accuracy, bias, safeguarding, intellectual property, data protection and professional judgement.

Users must:

- use only approved AI tools for Trust business where required by Trust guidance;
- check AI-generated outputs carefully before relying on them;
- ensure that professional judgement and human oversight are maintained;
- avoid entering confidential, personal, safeguarding, HR, financial, legal or commercially sensitive information into AI tools unless the tool has been approved for that purpose;
- avoid uploading pupil personal data or special category data into AI tools unless expressly authorised and risk assessed;
- make clear where AI has materially contributed to pupil-facing or public-facing content where appropriate;
- comply with the Trust AI Policy.

Users must not:

- use AI to make final decisions about pupils, staff, recruitment, safeguarding, discipline, SEND, finance or governance without human oversight;
- use AI outputs without checking accuracy;
- enter confidential case information into unapproved tools;
- use AI to generate misleading, discriminatory, harmful or inappropriate content;
- use AI in a way that undermines academic integrity, professional standards or safeguarding duties.

Where AI is used for planning, drafting, summarisation or analysis, the user remains responsible for the final content and any decisions made.

---

23. Cloud Storage, File Sharing and Collaboration Platforms

Users must use approved Trust platforms for storing and sharing Trust information.

Users must:

- store Trust documents in approved locations such as SharePoint, OneDrive, Teams or other authorised systems;
- apply appropriate access permissions;
- check sharing links before sending;
- avoid “anyone with the link” sharing unless authorised;
- remove access when no longer required;
- avoid storing Trust records in personal cloud accounts;
- ensure version control and retention requirements are followed.

Users must not:

- store Trust information in personal Google Drive, Dropbox, iCloud or other personal accounts;
- share confidential information through unapproved platforms;
- grant access to people who do not need the information;
- download large quantities of Trust data without authorisation;
- remove Trust records from approved systems without permission.

---

24. Remote Working

Where users work remotely, they must ensure that Trust information remains secure.

Users must:

- use secure internet connections;
- avoid public or unsecured Wi-Fi unless using approved protection;
- prevent family members or others from viewing Trust information;
- ensure paper records are kept secure;
- avoid discussing confidential matters where they may be overheard;
- use Trust-approved systems;
- report device loss, theft or suspected compromise immediately.

Users must not:

- leave devices or papers unattended in public places;
- print confidential documents at home unless necessary and secure;
- dispose of Trust papers in household waste;
- use shared family devices for confidential Trust work unless authorised and secured.

---

25. Software, Apps and Licences

Users must only use software, apps, browser extensions and digital tools that are authorised for Trust use.
Users must not:

- install unauthorised software;
- use unlicensed software;
- download cracked, pirated or unofficial software;
- use personal subscriptions to process Trust data without authorisation;
- connect unauthorised apps to Trust systems;
- agree to online terms on behalf of the Trust unless authorised.

Requests for new software or digital tools must follow the Trust's procurement, data protection and cyber security approval process.

---

26. Cyber Security Expectations

All users must take responsibility for cyber security.
Users must:

- complete required cyber security training;
- be alert to phishing, impersonation and suspicious emails;
- report suspicious emails and links immediately;
- verify unusual payment, bank detail or procurement requests;
- challenge unexpected requests for confidential information;
- keep devices updated;
- use multi-factor authentication where required;
- protect passwords;
- follow ICT instructions.

Users must not:

- click suspicious links;
- open unexpected attachments from unknown or suspicious sources;
- provide passwords, authentication codes or payment details in response to unsolicited requests;
- ignore security warnings;
- disable antivirus, firewall, filtering or security settings;
- connect unauthorised devices to Trust systems.

Cyber security concerns must be reported immediately to ICT support and the relevant senior leader.

---

27. Financial Systems, Fraud Prevention and Public Funds

Users with access to finance, payroll, procurement or banking-related systems must exercise particular care.
Users must:

- comply with Finance Regulations and internal controls;
- use only authorised systems and approval routes;
- protect financial information;
- verify changes to supplier or employee bank details;
- report suspected fraud, phishing or mandate fraud immediately;
- comply with segregation of duties;
- keep audit trails complete and accurate.

Users must not:

- share finance system logins;
- approve transactions outside authority limits;
- bypass procurement rules;
- alter records without proper authorisation;
- conceal errors, conflicts of interest or suspected irregularities.

Misuse of finance or payroll systems may be treated as gross misconduct and may be referred to external agencies.

---

28. Records, Retention and Disclosure

Trust records must be managed in accordance with legal, regulatory and operational requirements.
Users must:

- store records in approved systems;
- retain records for required periods;
- avoid unnecessary duplication;
- preserve records where litigation, investigation, audit, SAR, FOI or safeguarding matters are anticipated;
- dispose of records securely when authorised.

Users must not:

- delete, destroy or conceal records to avoid disclosure;
- remove Trust records without authorisation;
- store key Trust records only in personal folders or individual mailboxes where this may affect business continuity;
- use messaging platforms as a substitute for proper record keeping.

Messages, emails, documents, Teams chats and other digital records may be disclosable in response to subject access requests, freedom of information requests, audits, investigations, complaints, legal proceedings or regulatory requirements.

---

29. Recording, Images, Video and Audio

Users must comply with safeguarding, data protection and consent requirements when taking, storing or sharing images, video or audio.
Users must not:

- record meetings, pupils, staff or parents without appropriate authority;
- take images or videos of pupils on personal devices unless specifically authorised;
- share images externally without permission;
- upload images, audio or video to unapproved platforms;
- use covert recording except where expressly authorised and lawful.

Where meetings are recorded or transcribed, participants should normally be informed unless there is a lawful and exceptional reason not to do so.

---

30. Contractors, Consultants and Third Parties

Contractors, consultants and third parties may only access Trust systems, information or networks where authorised.
The Trust must ensure that appropriate arrangements are in place, including where relevant:

- confidentiality obligations;
- data processing agreements;
- cyber security requirements;
- safeguarding checks;
- access restrictions;
- account expiry dates;
- contract clauses;
- return or deletion of data on completion.

Third-party access must be limited to what is necessary and removed when no longer required.

---

31. Access Rights, Starters, Movers and Leavers

The Trust will manage user access according to role and need.
Access rights must be:

- approved before being granted;
- limited to role requirements;
- reviewed periodically;
- amended promptly when roles change;
- removed promptly when employment or engagement ends.

Line managers and school leaders must notify ICT support promptly of starters, movers, leavers, suspensions, long-term absence and role changes.
When a user leaves the Trust, the Trust may access, preserve, redirect, archive or delete information in the user's account as required for business continuity, legal, safeguarding, audit, data protection or operational purposes.

---

32. Suspension, Investigation or Absence

Where a user is suspended, absent or subject to investigation, the Trust may restrict or remove access to Trust systems, devices and accounts.
The Trust may also:

- secure devices;
- preserve email accounts and records;
- prevent deletion or alteration of information;
- review access logs;
- retrieve Trust information;
- access relevant mailbox content;
- redirect incoming business communications;
- appoint authorised individuals to manage operational continuity.

Such action must be proportionate, documented and authorised.

---

33. Incident Reporting

Users must immediately report:

- suspected data breaches;
- lost or stolen devices;
- misdirected emails containing personal or confidential information;
- unauthorised access;
- suspected phishing or malware;
- suspected fraud or financial irregularity;
- inappropriate online content;
- safeguarding concerns;
- accidental access to inappropriate websites;
- compromised passwords;
- suspicious system behaviour;
- any breach of this policy.

Reports should be made to the user's line manager, headteacher, ICT support, Data Protection Officer, safeguarding lead or Chief Financial Officer as appropriate.
Where safeguarding is involved, safeguarding procedures must be followed immediately.

---

34. Data Breaches

A data breach may include:

- sending personal data to the wrong recipient;
- losing a device or paper records;
- unauthorised access to personal data;
- accidental deletion or alteration of data;
- cyber attack;
- ransomware;
- inappropriate disclosure;
- sharing confidential information without authority.

All suspected breaches must be reported immediately. Users must not attempt to conceal or delay reporting a breach.
The Trust will assess breaches in accordance with data protection legislation and determine whether notification to the ICO, affected individuals or other bodies is required.

---

35. Monitoring, Audit and Compliance

The Trust may monitor and audit compliance with this policy.
This may include reviewing:

- security logs;
- access logs;
- internet activity;
- email records;
- file access;
- device compliance;
- cloud storage permissions;
- system alerts;
- filtering and monitoring reports;
- account activity;
- software usage;
- data transfer activity.

Monitoring will be carried out for legitimate purposes and must be lawful, necessary and proportionate.
Records of monitoring or access may be used in safeguarding, HR, disciplinary, audit, cyber security, data protection, legal or operational processes.

---

36. Breaches of this Policy

A breach of this policy may result in one or more of the following:

- advice, guidance or retraining;
- withdrawal or restriction of access;
- requirement to return equipment;
- management action;
- formal investigation;
- disciplinary action;
- dismissal;
- referral to the Local Authority Designated Officer where safeguarding thresholds may be met;
- referral to the police;
- referral to the ICO;
- referral to professional bodies;
- civil or legal action.

Serious breaches may be treated as gross misconduct.
Examples of potential gross misconduct may include:

- deliberate unauthorised access to confidential records;
- disclosure of safeguarding, HR, payroll, finance or pupil information without authority;
- accessing illegal or harmful material;
- deliberate data breach;
- deliberate bypassing of security controls;
- sharing passwords to enable unauthorised access;
- misuse of finance systems;
- use of Trust systems for fraud;
- harassment, bullying or discriminatory conduct using digital systems;
- deletion or concealment of records relating to an investigation;
- refusal to return Trust-owned equipment or information;
- deliberate misuse of AI tools involving confidential or personal data.

---

37. Training and Awareness

The Trust will ensure that users receive appropriate information, training and guidance on acceptable use, cyber security, data protection, safeguarding and online safety.
This may include:

- induction training;
- annual policy acknowledgement;
- cyber security awareness training;

- safeguarding training;
- data protection training;
- phishing awareness;
- online safety updates;
- AI use guidance;
- targeted training following incidents or changes in risk.

Users are required to complete mandatory training and comply with Trust instructions.

---

38. Policy Acknowledgement

This policy will be made available through the Trust's policy publication arrangements.
Use of Trust systems, devices, accounts, networks or information constitutes acceptance of this policy.
The Trust may require users to confirm electronically that they have read, understood and agree to comply with this policy. Failure to complete an acknowledgement does not remove the obligation to comply with the policy where the policy has been made available and communicated.
New starters, trustees, governors, volunteers, contractors and other users may be required to confirm acceptance before access is granted.

---

39. Equality, Inclusion and Accessibility

The Trust will apply this policy fairly and consistently.
Reasonable adjustments will be considered where a user has a disability or other need that affects their ability to access systems, complete training or comply with aspects of this policy.
The Trust will ensure that acceptable use expectations do not unfairly disadvantage users and that digital systems are used in a way that supports inclusion, accessibility and dignity.

---

40. Review

This policy will be reviewed annually, or sooner where required due to:

- changes in legislation;
- changes in DfE, ICO or safeguarding guidance;
- cyber incidents;
- data breaches;
- significant operational changes;
- new systems or technology;
- audit findings;
- safeguarding concerns;
- governance review;
- Trust growth or school conversion;
- lessons learned from incidents.

Appendix 1: Optional User Declaration and Acknowledgement

The completion of this declaration is not mandatory for the policy to apply. The Trust may use this declaration as part of induction, annual policy assurance, ICT account issuance, governance compliance processes or specific staff training programmes.

Acceptable Use Policy Acknowledgement

I confirm that:

- I have read and understood the ACT Multi Academy Trust Acceptable Use Policy.
- I understand my responsibilities when using Trust systems, devices, networks, software, digital platforms and information.

- I understand that all Trust systems, devices, email accounts, records and data are provided for legitimate Trust purposes.
- I understand that information held within Trust systems may be accessed, monitored, retrieved, preserved or reviewed where the Trust has a lawful, legitimate and proportionate reason to do so.
- I understand my obligations relating to safeguarding, cyber security, confidentiality, data protection and professional conduct.
- I understand that breaches of the Acceptable Use Policy may result in management action, disciplinary action, removal of system access, referral to professional bodies and/or referral to external agencies where appropriate.
- I agree to comply with the requirements of the Acceptable Use Policy and any associated Trust procedures.

Declaration	Details
Full Name	
Position	
School / Department	
Signature (if applicable)	
Date	

Electronic Acknowledgement
Where this policy is published through a policy management system, payroll portal, SharePoint site, intranet or learning platform, electronic acceptance may be accepted in place of a physical signature.
Electronic acknowledgement shall be deemed equivalent to a signed declaration for the purposes of evidencing awareness and acceptance of the policy requirements.

Appendix 2: Mailbox Access Authorisation Record

This form should be used where access to a Trust email account or mailbox is required for business continuity, safeguarding, HR, legal, data protection, finance, audit, investigation or operational purposes.

Item	Detail
Name of mailbox/account	
Account holder role/school	
Reason for access	
Legal/operational basis	
Is the account holder absent, suspended, departed or under investigation?	
Is safeguarding involved?	
Is HR/disciplinary involved?	
Is finance/payroll/procurement involved?	
Is DPO advice required?	
Authorising officer	
Date and time authorised	
Person carrying out access/search	
Search terms/folders/date range used	
Information retrieved	
Personal/unrelated information encountered?	
How was irrelevant personal information minimised?	
Where retrieved records were stored	
Date access completed	

Item	Detail
Follow-up action required	

Appendix 3: Acceptable Use Quick Guide for Staff

Staff must:

- use Trust systems professionally;
- keep passwords secure;
- use Trust email for Trust business;
- protect pupil, staff, safeguarding, HR and finance information;
- report breaches, phishing, lost devices and concerns immediately;
- use only approved systems and platforms;
- maintain professional boundaries online;
- check recipients carefully before sending emails;
- use AI only in accordance with Trust guidance;
- remember that Trust systems and email accounts may be accessed where there is a legitimate reason.

Staff must not:

- share passwords;
- use personal email for Trust business;
- store Trust data in personal cloud accounts;
- bypass filtering or monitoring;
- upload confidential information to unapproved AI tools;
- access records without a role-based reason;
- disclose confidential information without authority;
- use Trust systems for inappropriate, offensive, illegal or excessive personal activity;
- delete or conceal records relevant to an investigation, audit, request or complaint.

Appendix 4: Serious Incident Escalation Route

Type of Concern	Immediate Action	Notify
Safeguarding / child protection concern	Follow safeguarding procedures immediately	DSL / Headteacher / Trust Safeguarding Lead
Data breach	Contain breach and report immediately	DPO / CFO / Headteacher
Cyber incident / suspected malware	Disconnect if advised, do not investigate alone	IT Support / CFO
Lost or stolen device	Report immediately	IT Support / DPO / Line Manager
Suspected fraud or financial irregularity	Preserve evidence and escalate	CFO / CEO
Staff misuse / misconduct	Preserve evidence and seek advice	Headteacher / CEO / HR
Mailbox access required	Complete authorisation record	CEO / CFO / DPO as appropriate
Illegal content or criminal concern	Do not copy or share content	DSL / CEO / Police as appropriate

Appendix 5: Relationship with Other Policies

This policy should be read alongside:

- Data Protection Policy;
- Cyber Security Policy;
- Safeguarding and Child Protection Policy;
- Online Safety / Filtering and Monitoring Policy;
- Staff Code of Conduct;
- Disciplinary Policy;

- Whistleblowing Policy;
- AI Policy;
- Finance Regulations;
- Fraud and Anti-Bribery Policy;
- Records Management and Retention Policy;
- Freedom of Information Policy;
- Business Continuity Plan;
- Remote Working Policy, where applicable;
- Laptop / Device Agreement, where applicable.

Where there is any conflict between this policy and a more specific safeguarding, data protection, HR, finance or legal requirement, the Trust will apply the requirement that provides the highest level of protection and compliance.