MARK Education Trust

Acceptable Use Policy for Staff and Students

Policy document provenance

Approver:	Main Trust Board
Date of approval:	November 2025
Reviewer:	IT and Systems Link Trustee
Policy owner:	Trust Central Team
Policy author(s):	Head of IT
Date of next review:	September 2026 (to ensure it is aligned with updated KCSIE)

Version Control:	V1.0 November 2025
Summary of key changes made since last review:	Formatting updates to bring in line with the trust's policy template. Full revision of policy and process to ensure it aligns with KCSIE 2025.

Unless there are legislative or regulatory changes in the interim, this policy will be reviewed on an annual basis. Should no substantive changes be required at this point, the policy will move to the next review cycle

Related policies:	MARK Education Trust Online Safety Policy MARK Education Trust Cyber Security Policy MARK Education Trust Safeguarding & Child Protection Policy MARK Education Trust Staff Code of Conduct MARK Education Trust Data Protection and GDPR Policy

1. Staff ICT Acceptable Use Policy (AUP)

1.1 Equipment principles

MARK Education Trust is committed to safeguarding its ICT infrastructure to ensure it can be used effectively to support teaching, learning, and administrative processes. Ensuring the safety and integrity of the academy's ICT infrastructure is the shared responsibility of all staff.

Staff are encouraged to make full and appropriate use of the ICT infrastructure and mobile devices, including laptops, tablets, and mobile phones, in a **responsible, secure, and professional** manner.

By using academy ICT systems, devices, and accounts, staff agree to follow the terms of this policy, related safeguarding procedures, and data protection legislation. Misuse may result in disciplinary action and, in some cases, legal proceedings.

Ignorance of this policy is not an acceptable excuse in cases of misuse. All staff receive this policy during induction and must remain updated on any changes.

1.2 Purpose

- To protect the academy networks, systems, and equipment.
- To protect academy and personal data.
- To safeguard students, staff, and the wider community.
- To reduce the risk of legal action arising from misuse.
- To ensure compliance with **Keeping Children Safe in Education (KCSIE) 2025**, the Children Act 2004, GDPR, and the DfE Digital Standards for Education' Standards.

1.3 Password and account security

- Staff will receive a secure User ID and initial password at induction. Passwords must **not be shared** with any other individual.
- Default passwords must be changed immediately upon account activation.
- Complex passwords must be used containing at least three different character types and be at least 8 characters long.
- If a password or account is compromised, IT support must be notified immediately.
- **Multi-factor authentication** (MFA) must be used where available.
- A logged in device should never be left unattended.

1.4 General conditions of use

Staff use of ICT must:

- Be for professional and for educational purposes.
- Comply with legal and statutory safeguarding responsibilities.
- Not interfere with others' use of ICT facilities.
- Respect copyright, intellectual property, and licensing laws.
- Not involve unauthorised access, file sharing, or software installation.
- Not be used for harassment, bullying, defamation, hate speech, intimidation, or abuse.
- Not be involved in creating, accessing or distributing obscene, extremist, illegal, or discriminatory content.
- Not bring the trust or its academies into disrepute.
- Not use Personal accounts or devices to store or share academy data unless explicitly authorised and secured.
- Not Transmit threatening, defamatory, or illegal content.

- Not Access unauthorised systems or data.
- Impair IT system performance.
- Not Use AI or online platforms to process personal/sensitive data.
- Not use equipment for private financial gain or commercial activity.
- Report any faults, damage, or breaches immediately to ICT Support.
- Not disable, damage, or misuse ICT systems, intentionally or accidentally.
- Not remove\relocated any hardware internally or externally without prior approval from IT Support. Removing equipment off site requires SLT approval and a loan agreement must be signed. Any loaned equipment must be returned when no longer required.
- Not attempt to bypass filtering or security systems.

1.5 Use of Artificial Intelligence (AI)

- Staff may use AI tools to support teaching, learning, and administrative efficiency **only in line with safeguarding, data protection, ethical guidelines, MARK Education Trust AI Charter and MARK Education Trust values**.
- **No personal, sensitive, or identifiable information** about students, staff, or parents must ever be entered into AI systems without prior SLT authorisation.
- AI must not be used to generate or distribute inappropriate, discriminatory, or misleading content.
- Use of AI must align with the academy's curriculum aims and safeguarding responsibilities as set out in **KCSIE 2025**.
- Staff remain accountable for any outputs used from AI tools. All outputs should be reviewed before using.

1.6 Data security

- Sensitive and personal data must only be accessed through secure trust systems (e.g., Microsoft 365, remote access).
- Staff must keep **all student and staff data confidential**, except where law or policy requires disclosure to an appropriate authority.
- Data must not be stored locally on personal devices.
- Data must be stored on a secure, trust approved platform (e.g. Microsoft 365). Storing any materials in personal accounts is strictly prohibited.
- Staff must comply with GDPR, Data Protection Act 2018, and trust procedures.
- Any data breach must be reported immediately in line with the academy's Data Breach Procedure.

1.7 Anti-virus and firewall protection

- All academy devices and personal devices are protected with up-to-date security software and patches.
- Staff must not alter security configurations.
- Suspected malware or virus infections must be reported to IT support as soon as possible.
- Compromised devices may be temporarily disconnected by IT staff (or instructed to by IT staff) from the network until resolved.

1.8 Physical security

- ICT equipment must be handled with care and securely stored when not in use.
- Portable devices must never be left unattended or visible in vehicles.
- Liquids must be kept away from ICT equipment.
- Staff supervising students must always ensure appropriate use of equipment.

1.9 Monitoring and logging

- Network and internet activity may be monitored and logged for safeguarding, security, and audit purposes.
- Logs are stored securely and retained only as long as necessary in line with GDPR and the trust's Data Retention policy.
- The trust may be required by law to share logs with external authorities.

2. Use of email and internet by staff

2.1 Principles

Email and internet access are provided primarily to support professional practice. Limited personal use may be permitted, but all activity must comply with this policy, safeguarding guidance, GDPR, and trust procedures.

This policy aligns with the **Human Rights Act**, **Data Protection Act**, and **KCSIE 2025**, and ensures a balance between staff privacy and safeguarding obligations.

2.2 Email guidelines

- Emails must be written professionally and respectfully
- Defamatory, offensive, harassing, obscene, or discriminatory content is prohibited
- Suspicious attachments or phishing attempts must be reported to ICT immediately
- The academy reserves the right to audit and access email accounts when misuse is suspected or during prolonged absences
- Forwarding inappropriate content may result in disciplinary action.

2.3 Internet guidelines

- Internet use must support educational and professional purposes
- Personal use must be minimal, lawful, and appropriate
- Viewing or distributing illegal, extremist, pornographic, or discriminatory material is strictly prohibited
- The academy reserves the right to monitor and audit browsing activity.

2.4 Personal devices

- No Academy data may be stored locally on personal devices
- Devices used to access Academy data/resources must have up-to-date security patches/updates and passcodes
- Personal device use during work time must not impact professional responsibilities
- AI or cloud services accessed from personal devices must comply with data protection and safeguarding.

2.5 Software use

- Software must be correctly licensed for education use
- Installation of software must be approved by IT support
- Unauthorised installation or use of unlicensed software may result in disciplinary action
- Unauthorised updating or removal of software is prohibited.

2.6 Reporting and safeguarding

- Any concerns related to online behaviour, cyber incidents, or suspected safeguarding breaches must be reported immediately to the Designated Safeguarding Lead (DSL)

- This includes incidents involving social media, online harassment, and the misuse of AI or digital platforms
- This aligns with **DfE Digital standards** and **KCSIE 2025** requirements for early reporting and intervention
- Discovery of illegal or harmful material must be reported to **Senior Leadership** as soon as possible
- Accidental access to inappropriate material must be reported immediately.

2.7 CCTV

Viewing and monitoring CCTV footage **must** only be carried out by specified staff for the following purpose only:

- Safeguarding
- Security
- Investigations approved by SLT.

2.8 Breaches of this policy

Breaches are classified as **minor**, **moderate**, or **severe**, with appropriate disciplinary action:

- **Minor Breach:** verbal warning; logged for 12 months
- **Moderate Breach:** formal sanction; possible restriction of ICT access
- **Severe Breach:** potential dismissal, restriction of ICT access, and legal action.

Examples of a breach include, but are not limited to:

- Sharing login details, using another's credentials
- Accessing inappropriate content
- Breaching data protection or safeguarding
- Introducing malware or unauthorised software
- Deliberate misuse of AI tools
- Use of CCTV outside of the stated purpose.

Investigations will be carried out by Senior Leadership under the direction of the Headteacher, following the academy's disciplinary procedures.

2.9 This acceptable use policy must be read in conjunction with:

- KCSIE 2025
- Data Protection and GDPR Policy
- Safeguarding and Child Protection Policy
- Online Safety Policy
- Staff Code of Conduct.

3. Student ICT Acceptable Use policy (AUP)

All students must follow the conditions described in this and any other Acceptable Use Policy of MARK Education Trust when using both school and personal ICT devices and accounts. Students will receive guidance from staff in the appropriate and safe use of these resources, but any use of MARK Education Trust accounts remains the personal responsibility of the user.

The trust is committed to providing a safe and secure digital environment for students, in line with **Keeping Children Safe in Education (KCSIE) 2025**, the **Online Safety Act 2023**, and DfE Digital Standards.

3.1 Conditions of use

Student access to digital resources is a **privilege, not a right**. Students are expected to use these resources responsibly and for **educational purposes only**. Every student must take all reasonable steps to ensure they comply with the conditions of this and any other Acceptable Use Policy.

The school uses filtering and monitoring systems in line with **DfE and KCSIE 2025** standards to help keep students safe online, but each student remains responsible for their own actions.

3.2 Acceptable use

Students are expected to use school systems safely, legally, and responsibly. You must:

- Ensure your personal device (if used to access school systems) has **up-to-date antivirus protection** and latest security patches
- Use ICT equipment only for **educational purposes**. Activities such as buying, selling, or promoting goods and services are not permitted
- Always check removable media (e.g., USB sticks, CDs) for malware before using them. You can do this by scanning the media before opening any files through the anti-virus software installed.
- Only access websites, applications, and platforms that are appropriate and have been agreed by a member of staff
- Use appropriate and respectful language when using any school ICT systems
- Never use ICT to participate in illegal, extremist, discriminatory, or harmful activities.
- Obtain **explicit permission** before recording any student, adult, or activity using sound, photo, or video
- Not upload or share any text, image, sound, or video intended to **harass, bully, embarrass, or distress** others in the school or wider community
- Not share or use hate speech, extremist content, conspiracy theories, or misinformation/disinformation as defined in KCSIE 2025
- Protect your personal information and that of others (e.g., do not share addresses, phone numbers, or logins)
- Never share your login details or use another person's username or password
- Never leave a logged in device unattended
- Not attempt to bypass school **filtering or monitoring systems**
- Not download or view inappropriate, extremist, or illegal material
- Not damage, alter, or tamper with equipment or another user's work
- Seek permission before installing or storing programs or apps on school devices
- Keep food and drink away from ICT equipment to prevent damage.

3.3 Use of Artificial Intelligence (AI) tools

Students may have access to AI tools (e.g., generative AI for text, images, or other digital content) as part of their learning.

AI use at MARK Education Trust must follow these rules:

1. **Educational purpose only**
   - AI tools may **only be used for learning tasks** approved by a teacher or staff member
   - Students must not use AI to cheat, plagiarise, or create misleading content.
2. **No sensitive or personal data**
   - Students **must never input personal, sensitive, or confidential information** (about themselves, other students, staff, or the school) into AI tools
   - This includes names, addresses, phone numbers, passwords, exam content, medical information, or any other data that could identify an individual.
3. **Responsible use and supervision**
   - AI content generated must be **reviewed by staff** before submission or publication
   - Students must not create content intended to harass, embarrass, misinform, or harm anyone.
4. **Attribution and plagiarism**
   - Work generated by AI should **clearly acknowledge AI assistance** if it forms part of an assignment or project
   - Students remain responsible for ensuring work is original, accurate, and appropriate.
5. **Cybersecurity and compliance**
   - AI tools used must be **approved by the school**, meet security standards, and comply with data protection rules
   - Attempts to bypass school systems to access unapproved AI tools are prohibited.

3.4 Unacceptable use

Unacceptable use includes, but is not limited to:

- Violating the privacy, dignity, or safety of others
- Creating, transmitting, or sharing content likely to harass, offend, distress, or cause anxiety.
- Bringing the trust or school into disrepute
- Attempting to access or distribute extremist, violent, sexual, or illegal material
- Attempting to bypass security, filtering, or monitoring systems
- Engaging in online bullying, intimidation, trolling, or harassment
- Using AI tools to impersonate, spread false information, or harass others

Note: All network and device activity is monitored and logged in line with KCSIE 2025 and DfE filtering and monitoring standards. Misuse can and will be traced.

3.5 Sanctions

If a student fails to comply with this policy, their internet, email, and/or computer access may be restricted or withdrawn.

Breaking the Student AUP may lead to:

- Withdrawal or suspension of network or internet access
- Increased monitoring of network activity
- Investigation of past network usage
- Behaviour or safeguarding sanctions, including suspension or exclusion
- Referral to external agencies such as the **police or local authority** where appropriate

- Where a safeguarding concern is identified, it will be handled according to the trust's Child Protection and Safeguarding Policy.

3.6 Social media & cyberbullying

The trust takes **cyberbullying**, **misuse of social media**, and **online harms** very seriously. Students must:

- Not use social media in ways that harass, bully, or harm others.
- Respect age restrictions on platforms:
  - Facebook – 13 years
  - Instagram – 13 years
  - Twitter/X – 13 years
  - TikTok – 13 years
  - Snapchat – 13 years
- Not impersonate others or share content designed to spread misinformation or hatred.

Parents who allow children to use social media below the minimum age accept responsibility for issues arising from that use. School support may be limited where platforms are used outside the trust's jurisdiction.

3.7 Use of ICT and the law

Use of ICT leaves a **digital footprint** which can be traced. Inappropriate or illegal activity may be reported to law enforcement.

Relevant legislation includes:

- Protection from Harassment Act 1997
- Malicious Communications Act 1988
- Communications Act 2003 (Section 127)
- Public Order Act 1986
- Defamation Acts 1952 & 1996
- Computer Misuse Act 1990
- Crime and Disorder Act 1998
- Police and Justice Act 2006
- Online Safety Act 2023

Misusing ICT can be a **criminal offence**.

3.8 Support, education & safeguarding

- The school will provide regular digital literacy and online safety education, including awareness of misinformation, AI, online grooming, cybersecurity, and digital wellbeing in line with KCSIE 2025
- Students are encouraged to report concerns immediately to a trusted adult, teacher, or the Designated Safeguarding Lead (DSL)
- The school uses filtering and monitoring technology that complies with DfE standards and is reviewed annually
- Students placed in alternative provision remain under the trust's safeguarding responsibilities.