EQUITAS ACADEMIES TRUST

ICT & INTERNET ACCEPTABLE USE POLICY (AUP)

Review Date: **March 2026**

To be Reviewed: **March 2028**

Agreed: **F & GP Committee**

Policy Lead: **Strategic IT and Network Manager**

1. Introduction and aims

Information and communications technology (ICT) is an integral part of the way our trust works, and is a critical resource for pupils, staff (including the senior leadership team), governors, volunteers, and visitors. It supports teaching and learning, and the pastoral and administrative functions of the trust.

However, the ICT resources and facilities our trust uses could also pose risks to data protection, online safety and safeguarding. This policy aims to:

- Set guidelines and rules on the use of Trust ICT resources for staff, pupils, parents and governors
- Establish clear expectations for the way all members of the community engage with each other online
- Support the trust's policies on data protection, online safety and safeguarding
- Preventing disruption that could occur to the trust through the misuse, or attempted misuse, of ICT systems
- Support the trusts in teaching pupils safe and effective internet and ICT use

This AUP also sets out our expectations for the safe and ethical use of Artificial Intelligence (AI), including generative AI tools (e.g., Microsoft Copilot). Staff and pupils must not input personal, sensitive or confidential data into generative AI tools, and AI must never replace professional judgement. See the Trust AI Policy (2024) and Staff AI Usage Agreement (2025).

This policy covers all users of our trust's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors. Breaches of this policy may be dealt with under our staff behaviour policy.

2. Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance (latest versions at the URLs provided):

- Data Protection Act 2018; UK General Data Protection Regulation (UK GDPR)
- Computer Misuse Act 1990; Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011; Education and Inspections Act 2006; Freedom of Information Act 2000
- Keeping Children Safe in Education (KCSIE) 2024/2025: https://www.gov.uk/government/publications/keeping-children-safe-in-education--2
- Searching, Screening and Confiscation (DfE) 2023: https://www.gov.uk/government/publications/searching-screening-and-confiscation

- UKCIS guidance on sharing nudes and semi-nudes (updated 2024): https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people
- Online Safety Act 2023 (and Ofcom codes and guidance 2024–2025): https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer
- DfE: Generative artificial intelligence (AI) in education (updated 2025): https://www.gov.uk/government/publications/generative-artificial-intelligence-in-education/generative-artificial-intelligence-ai-in-education
- JCQ (2025) Artificial Intelligence Use in Assessments: https://www.jcq.org.uk/knowledge-hub/ai-use-in-assessments-your-role-in-protecting-the-integrity-of-qualifications/
- National Cyber Security Centre (NCSC): Cyber Security for Schools: https://www.ncsc.gov.uk/section/education-skills/cyber-security-schools | Exercise in a Box: https://www.ncsc.gov.uk/information/exercise-in-a-box
- DfE: Meeting digital and technology standards in schools and colleges (updated 2026): https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges
- Education and Training (Welfare of Children) Act 2021: https://www.legislation.gov.uk/ukpga/2021/16/enacted

Trust links: This AUP should be read alongside the Trust AI Policy (2024), Staff AI Usage Agreement (2025), Data Protection Policy, Online Safety Policy, Behaviour Policy and Safeguarding/Child Protection Policy.

3. Definitions

ICT facilities: all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the trust's ICT service

Users: anyone authorised by the trust to use the trust's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors

Personal use: any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user

Authorised personnel: employees authorised by the trust to perform systems administration and/or monitoring of the ICT facilities

Materials: files and data created using the trust's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

Artificial Intelligence (AI): technologies that perform tasks typically requiring human intelligence;
Generative AI: AI systems that create new content (text, images, audio, code, video).
'Pupil-facing AI' refers to any AI interacted with directly by pupils.

4. Unacceptable use

The following is considered unacceptable use of the trust's ICT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings. Unacceptable use includes, but is not limited to:

- Breaching intellectual property rights or copyright
- Bullying or harassment, or promoting unlawful discrimination
- Any illegal conduct, or statements advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Activity which defames or disparages the trust, or risks bringing the trust into disrepute
- Sharing confidential information about the trust, its pupils, or other members of the community
- Connecting any device to the trust's ICT network without approval from authorised personnel
- Setting up software, applications or web services on the trust's network without approval, or creating/using any software designed to interfere with the functioning of the trust's ICT facilities, accounts or data
- Gaining (or attempting to gain) unauthorised access to restricted areas of the network or any password-protected information
- Allowing, encouraging or enabling others to gain unauthorised access
- Causing intentional damage to the trust's ICT facilities, or removing/deleting/disposing of trust equipment, systems, programmes or information without permission
- Causing a data breach by accessing, modifying, or sharing data (including personal data) without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless directly related to the trust
- Using websites or mechanisms to bypass the trust's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way

AI-specific unacceptable use (additional to the above):

• Entering personal, sensitive or confidential information (including student, staff or parent data; commercially sensitive information; or intellectual property) into generative AI tools

• Uploading pupil work to AI platforms without appropriate consent and/or a lawful basis; failing to follow DPIA outcomes

• Using AI to generate or disseminate harmful, abusive, extremist, pornographic or deceptive content (including deepfakes and impersonation)

• Using AI to evade academic integrity (e.g., producing assessed work, or significant portions of it, without acknowledgement in line with JCQ and awarding-body rules)

• Using unapproved AI tools or browser extensions that collect data without appropriate safeguards

- Use of VPNs, anonymous browsers, or other circumvention tools to bypass filtering/monitoring.

4.1 Exceptions from unacceptable use

Where use is required for a legitimate educational, research or safeguarding purpose that would otherwise be unacceptable, exemptions may be granted at the headteacher's discretion. Staff/students must request permission by email, explaining the purpose.

4.2 Sanctions

Pupils and staff who engage in unacceptable activity may face disciplinary action in line with trust policies on behaviour and conduct. Access to the trust ICT facilities may be revoked.

5. Staff (including governors, volunteers and contractors)

5.1 Access to trust ICT facilities and materials

The Strategic ICT Network & Systems Manager manages access to ICT facilities and materials, including devices and permissions. Staff will be provided with unique credentials and must use them when accessing trust facilities. Access issues should be raised with IT Support.

5.2 Use of phones and email

The trust provides each member of staff with an email address for work purposes only. Staff must enable multi-factor authentication. Work-related business must be conducted using the trust email. Personal contact details must not be shared with pupils or parents.

Sensitive or confidential information sent by email must be encrypted. Mis-sent emails containing personal data must be reported immediately in line with the data breach procedure.

5.3 Personal use

Occasional personal use of trust ICT facilities is permitted provided it does not occur during teaching hours, constitute unacceptable use, or interfere with work/learning. Personal use may be monitored, and disciplinary action may be taken where breaches occur.

5.4 Personal social media accounts

Members of staff should ensure their use of social media is appropriate at all times and consistent with the staff code of conduct.

5.5 Remote access

Remote access to trust facilities is permitted under the same rules as on-site access. Staff must take precautions as required by the Strategic ICT Network & Systems Manager to avoid importing malware or compromising security. Confidential and personal data must be handled in line with the data protection policy.

5.6 Monitoring and filtering of the trust network and use of ICT facilities

To safeguard pupils and provide a safe environment to learn, the trust reserves the right to filter and monitor use of its ICT facilities and network (e.g., websites visited, bandwidth, email, logs and other communications), to the extent permitted by law. Effectiveness of filtering and monitoring will be regularly reviewed.

Filtering and monitoring arrangements will align with DfE digital and technology standards (filtering & monitoring, cyber security) and KCSIE online safety expectations. See: https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges .

5.7 Responsible use of Artificial Intelligence (AI) – staff

• AI can be used to support planning, resource creation, marking of objective items, and workload reduction. Staff remain responsible and accountable for any AI-generated content used in trust work.

• Do not input personal data, confidential information, or intellectual property into generative AI systems. Never upload pupil work without appropriate consent and a completed DPIA where required.

• Where AI has been used (e.g., report writing, analysis), staff must review, verify and adapt outputs; content must be accurate, impartial, safe, appropriate for the audience, and use British spelling and trust-aligned terminology.

• Use only IT-approved platforms; the preferred platform is Microsoft Copilot. Do not use unvetted AI tools, browser plug-ins or extensions that collect data.

• Be alert to bias, hallucinations, outdated content, and IP/copyright issues in AI outputs.

• AI must not be used to make solely automated decisions about individuals; staff must retain professional judgement.

• Comply with JCQ and awarding-body rules regarding AI in assessments and academic integrity.

- AI must not be used to follow “exam influencer” trends or create deceptive content that undermines academic integrity

Cross-references: Trust AI Policy (2024); Staff AI Usage Agreement (CAPITAL framework); Data Protection Impact Assessment process.

6. Pupils

6.1 Access to ICT facilities

Computers and equipment in the ICT suite and on portable trolleys are available to pupils under staff supervision. Specialist equipment must only be used under staff supervision. Sixth-form pupils may use computers independently for educational purposes.

6.2 Search and deletion

Under the Education Act 2011, the headteacher and authorised staff may search pupils and confiscate devices where there are reasonable grounds for suspicion. Where appropriate, incidents will be referred to the DSL and managed in line with DfE guidance on Searching, Screening and Confiscation and UKCIS guidance on sharing nudes and semi-nudes.

If a device is suspected to contain indecent images of a child, staff must not view, copy, print, share, store or save the image. Confiscate the device and report immediately to the DSL. Follow UKCIS (2024) procedures.

6.3 Unacceptable use of ICT and the internet outside of trust

The trust may sanction pupils for unacceptable conduct online at any time, even off-site, including bullying and harassment; sharing nude or semi-nude images; data breaches; unauthorised access; or other misconduct bringing the trust into disrepute.

6.4 Responsible use of AI – pupils

• Pupils may use age-appropriate AI tools for learning when directed and supervised. The purpose, boundaries and safety measures will be made clear by staff.

• Pupils must not enter personal data (e.g., names, contact details), sensitive information or images into AI tools.

• Pupils must not use AI to cheat or misrepresent their work. Where AI has assisted learning, pupils may be asked to acknowledge this in line with teacher instructions and awarding-body rules.

• Pupils will be taught about AI's capabilities, limitations, risks (e.g., bias, inaccuracy, deepfakes, scams) and how to evaluate AI outputs critically. Pupils must understand that AI-generated intimate images, even if fake, are harmful and treated as serious safeguarding incidents.

7. Parents

Parents do not have access to the trust's ICT facilities as a matter of course. Where parents work with the trust in an official capacity, access may be granted at the headteacher's discretion and this policy will apply.

8. Data security

The trust will maintain appropriate security to safeguard systems, staff and learners, including firewalls, security features, user authentication/MFA, anti-malware and backups. Procedures are reviewed periodically to keep up with evolving cyber threats.

8.1 Passwords

All users must set strong, unique passwords and keep them secure. Sharing account or password information may result in disciplinary action or access revocation.

8.2 Software updates, firewalls and anti-malware

Trust devices will be kept up-to-date with security patches and anti-malware. Users must not circumvent safeguards. Personal devices on the trust network must also meet these requirements.

8.3 Data protection

All personal data must be processed in line with data protection legislation and the trust's data protection policy.

8.4 Access to facilities and materials

Users will have clearly defined access rights. Unauthorised access must be reported immediately. Users should lock devices when unattended and log out/shut down at the end of each day.

8.5 Encryption

Trust devices and systems will have appropriate encryption. Staff may only use personal devices to access trust data where expressly authorised and where security/encryption meet trust standards.

8.6 AI and data protection (new)

• Do not input personal data or confidential information into generative AI tools.

• A DPIA may be required before adopting new AI tools or processing. Follow the Data Protection Policy and DPIA procedure.

• Where sign-up requires names or email addresses, assess data sharing risks and document controls.

9. Protection from cyber attacks

The trust will work with governors and IT to ensure cyber security receives appropriate time and resources; provide annual cyber training; maintain incident reporting and response procedures; conduct access reviews; enable MFA; maintain firewalls; and back up critical data off-network.

Controls will be proportionate, multi-layered, up-to-date, and regularly reviewed and tested. The incident response plan will be reviewed and exercised annually (e.g., NCSC 'Exercise in a Box') and, after significant events, reported where appropriate (e.g., Action Fraud/police, the ICO for qualifying personal data breaches).

10. Internet access

The trust's wireless connection is secure. Internet access is filtered and monitored, with separate connections for school devices, sixth form BYOD and guests, as configured by IT.

10.1 Parents and visitors

Parents and visitors will not be permitted to use the trust's Wi-Fi unless authorised by the headteacher for an official purpose. Staff must not share Wi-Fi passwords with unauthorised users.

10.2 Online Platforms & Services

The trust will ensure due-diligence and oversight of online platforms used in school, particularly around age-ratings, communication features and risks associated with user-generated content.

11. Monitoring and review

Headteachers and the Strategic ICT Network & Systems Manager monitor the implementation of this policy and ensure it is updated to reflect trust needs. This policy will be reviewed at least annually, or sooner if legislation/guidance changes materially (e.g., KCSIE, DfE Digital & Technology Standards, Ofcom Online Safety codes, DfE AI guidance). The governing board approves this policy.

Appendix A: Acceptable use agreement – older pupils (summary)

When using the trust's ICT and internet, I will not use them for non-educational purposes without permission; access inappropriate websites; use chat rooms without permission; open

suspicious emails; share nudes or semi-nudes; share passwords; or bully others. I understand the trust will monitor my use.

AI: I will not use AI tools to cheat or misrepresent my work. I will not enter my personal data or images into AI tools. I will follow teacher instructions and acknowledge permitted AI assistance when asked.

Appendix B: Acceptable use agreement – younger pupils (summary)

I will ask a teacher before using ICT; not go on inappropriate websites; not use chat rooms; not open links or attachments without checking; be kind in my messages; not send pictures of people without clothes; not share my password; tell a teacher if something online upsets me.

AI: If we use any AI tools in class, I will do so with my teacher and never share my personal information.

Appendix C: Acceptable use agreement – staff, governors, volunteers and visitors (summary)

I will not access inappropriate material; harm the trust's reputation; use improper language; install unauthorised software or connect unauthorised devices; share passwords; share confidential information; or access/modify/share data without authorisation. I understand monitoring applies and I will keep devices secure and data protected.

AI: I will follow the Trust AI Policy and Staff AI Usage Agreement (CAPITAL framework). I will not upload pupil work or personal data into AI tools; I will use only approved platforms; I will verify and adapt any AI outputs; and I will comply with JCQ and awarding-body rules regarding assessments.

Policy owner: Strategic ICT & Network Manager | Linked policies: AI Policy (2024), Staff AI Usage Agreement (2025), Data Protection, Online Safety, Safeguarding/Child Protection, Behaviour | Review: Annual or sooner if guidance changes.