Frank Field
Education Trust

ICT & Internet Acceptable Use Policy

Policy Information:

Date prepared	October 2026
Adopted by Board	October 2026
Implementation Date	Immediate
Frequency of Review	Bi-Annually
Review Date	October 2028

Approved by CEO:

Cath Green

Approved by Chair of Board:

David Wooff

Frank Field
Education Trust

Contents

Contents 2
1. Introduction and Aims 3
2. Legislation and Guidance 3
3. Scope and Definitions 3
4. Unacceptable Use 3
5. Sanctions and Consequences 4
6. Adult Users and Professional Responsibilities 4
7. Email, Phones and Electronic Communications 4
8. Personal Use and Social Media 4
9. Remote Access and Personal Devices 5
10. Filtering, Monitoring and Auditing 5
11. Pupils, Behaviour and Mobile Devices 5
12. Parents, Carers and Visitors 6
13. Data Security and Access Control 6
14. Data Protection and Records Management 6
15. Artificial Intelligence 6
16. Cyber Security and Incident Response 7
17. Internet and Wi-Fi Access 7
18. Roles and Responsibilities 7
19. Training, Monitoring and Review 7
20. Related Policies 8
Appendix 1: Social Media Guidance for Adult Users 9
Appendix 2: Parent and Carer Online Services Agreement 10
Appendix 3: Pupil Acceptable Use Agreement 11
Appendix 4: Adult User Acceptable Use Agreement 12
Appendix 5: Cyber Security Glossary 14

1. Introduction and Aims

Information and communications technology is integral to teaching, learning, safeguarding, administration, communication, and governance across Frank Field Education Trust. The Trust aims to ensure that technology is used lawfully, safely, professionally, and securely while supporting pupils and staff to benefit from digital services.

This policy sets consistent expectations for the use of Trust devices, accounts, networks, applications, cloud services, internet access, and information. It supports the Trust's Online Safety Policy, Data Protection Policy, safeguarding arrangements, records management framework, and cyber-security controls.

The policy also explains that Trust systems may be filtered, logged, monitored, reviewed, and audited where this is lawful, transparent, necessary, and proportionate.

2. Legislation and Guidance

This policy has been reviewed against the UK General Data Protection Regulation, Data Protection Act 2018 as amended by the Data (Use and Access) Act 2025, Computer Misuse Act 1990, Human Rights Act 1998, Equality Act 2010, Freedom of Information Act 2000, Education and Inspections Act 2006 and relevant provisions of the Education Act 2011.

The Trust also has regard to Keeping Children Safe in Education 2026, Department for Education guidance on searching, screening and confiscation, the statutory guidance on mobile phones in schools, the DfE digital and technology standards, including filtering, monitoring and cyber security, and relevant National Cyber Security Centre guidance.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 may be relevant to authorised monitoring of business communications. Monitoring will also be governed by data protection law, privacy information and the principles of necessity and proportionality.

3. Scope and Definitions

This policy applies whenever a person uses Trust ICT facilities, accesses Trust information, uses a Trust account, connects to a Trust network, or uses technology for a Trust-related educational, employment, governance, volunteering, or business purpose. It applies both on and away from Trust premises.

Users include pupils; employees; workers; agency, casual, temporary and supply staff; apprentices; trainees; consultants; contractors; trustees; governors; volunteers; work-experience personnel; visitors; parents and carers granted access; and any other person authorised to use Trust ICT facilities or information.

4. Unacceptable Use

Use is unacceptable where it is unlawful, unsafe, unauthorised, professionally inappropriate, or inconsistent with safeguarding, privacy, security, or the legitimate interests of the Trust. The Trust will consider the nature, context, seriousness, and effect of the conduct rather than relying only on a fixed list.

Unacceptable use includes unauthorised access; credential sharing; interference with security controls; connecting unapproved devices; installing software, browser extensions, or online services without approval; bypassing filtering or monitoring; deliberately damaging or deleting equipment, systems, or information; and using personal accounts or storage for Trust information.

It also includes bullying, harassment, discrimination, fraud, scams, unlawful gambling, misuse of copyright material, unauthorised disclosure, inappropriate recording, access to illegal or harmful

content, and the creation or distribution of manipulated or AI-generated material intended to impersonate, deceive, humiliate, harm or evade safeguards.

The Trust may permit an activity that would otherwise be restricted where it is necessary for a legitimate educational, safeguarding, legal, technical-security or operational purpose and has been approved in writing by an authorised senior leader. Conditions may be imposed and approval may be withdrawn.

5. Sanctions and Consequences

A breach may result in restriction, suspension, or withdrawal of access while the matter is considered. Any response will be proportionate to the facts, the user's status, and the applicable procedure.

Employees may be subject to management or disciplinary action. Contractors, agency staff, volunteers, and visitors may have access or their engagement withdrawn. Trustees and governors may be dealt with under governance arrangements. Pupils may be dealt with under the Behaviour Policy and safeguarding procedures. The Trust may also preserve evidence, make a safeguarding referral, notify a regulator, report a suspected offence, or take legal action where appropriate.

6. Adult Users and Professional Responsibilities

Access is granted according to role and legitimate need. Adult users must use only the accounts allocated to them, maintain professional boundaries, protect confidentiality and report concerns promptly. Access provided in error must not be used and must be reported to ICT support.

Trust equipment must be stored and transported safely and must not be left unattended in a public place or unsecured vehicle. Loss, theft, damage, or faults must be reported promptly. The Trust will establish the circumstances fairly before considering any recovery of cost, and any deduction from pay will only be made where contractually and legally permitted.

Adult users must use approved Trust channels for Trust business. Personal email, messaging, cloud storage, and social media accounts must not be used for Trust business unless a specific exceptional arrangement has been authorised.

7. Email, Phones and Electronic Communications

Users must communicate professionally and check recipients, attachments, sharing permissions, and sensitivity before sending information. Confidential or sensitive information must be shared through an approved secure method appropriate to the risk. Encryption or password protection must be used where instructed, with credentials communicated separately where necessary.

Information received in error must not be used or disclosed. The sender should be informed and the information deleted or returned as directed. An unintended disclosure must be reported immediately under the Trust's personal data breach procedure.

Electronic communications may be retrievable and disclosable in legal proceedings, safeguarding work, or information rights requests. Deleting a message from an inbox does not necessarily remove it from Trust systems.

Personal phone numbers and contact details must not normally be shared with pupils or parents. Work-related calls and messages must use approved Trust channels unless an authorised exception applies.

8. Personal Use and Social Media

Limited incidental personal use may be permitted where it does not interfere with work, teaching, learning, safeguarding, service availability, or security; does not incur material cost; does not involve

pupils; and does not include unlawful or unacceptable activity. Permission may be limited or withdrawn.

Users should understand that personal activity undertaken through Trust facilities may fall within lawful and proportionate filtering, logging, monitoring, retrieval, or audit.

Personal social media use must not undermine safeguarding, professional boundaries, confidentiality, working relationships or the Trust's reputation. Adult users must not accept or initiate personal social media connections with pupils and must not use personal accounts to conduct Trust business.

9. Remote Access and Personal Devices

Remote access must use approved devices, services, applications, and connection methods. Users must prevent unauthorised viewing, lock screens when unattended, avoid discussing confidential matters where they may be overheard and keep equipment and papers secure.

Trust information must not be downloaded to an unapproved device or copied to personal storage. A personal device may be used for Trust purposes only where expressly authorised and subject to specified technical and organisational controls. Personal devices must not be used to photograph, film or record pupils except under an expressly authorised arrangement using approved controls.

Where multi-factor authentication uses an approved application on a personal device, that use does not authorise the Trust to inspect or manage unrelated personal content. A suitable alternative should be considered where a user cannot reasonably use a personal device.

10. Filtering, Monitoring and Auditing

The Trust uses appropriate filtering and monitoring to safeguard pupils, protect users, systems, and information, prevent and detect misuse, maintain operational security, investigate concerns, and meet legal responsibilities. Filtering restricts access to illegal, inappropriate, or potentially harmful content. Monitoring may include staff supervision and technical systems that review activity, record relevant events, or generate alerts.

Monitoring will be lawful, fair, and transparent. The Trust will document the purpose, lawful basis, scope, access controls, retention arrangements and whether a Data Protection Impact Assessment is required. The least intrusive method reasonably capable of meeting the identified purpose will be used.

Users will receive appropriate information through this policy and relevant privacy notices. Covert monitoring will not be routine and may only be considered for a specific and limited purpose, with senior authorisation and appropriate legal and data protection advice.

The Trust Board will seek assurance that appropriate filtering and monitoring arrangements are in place. Effectiveness will be reviewed at least annually with input from the responsible senior leader, Designated Safeguarding Lead, and ICT support. Technical controls do not replace supervision, education, professional judgement, or safeguarding response.

11. Pupils, Behaviour and Mobile Devices

Pupils must use ICT responsibly, use only their own credentials, follow staff instructions, respect others, and report content, or contact that is harmful, worrying, or inappropriate. Pupil access will be age-appropriate, supervised where required and subject to applicable filtering and monitoring.

Any search of a pupil or device, confiscation of a device or deletion of data will be undertaken only by authorised staff and in accordance with the law, DfE guidance, the Behaviour Policy, and safeguarding procedures. Where material may be evidence of a criminal offence or safeguarding concern, staff must preserve it and seek advice rather than routinely viewing, copying, or deleting it.

In line with statutory guidance applying from 1 September 2026, the Trust expects schools to be mobile-phone-free environments by default throughout the school day. Each academy's Behaviour Policy or mobile-phone arrangements will identify any limited exceptions, including reasonable adjustments, medical needs, safeguarding arrangements or an approved Bring Your Own Device scheme for laptops or tablets. A BYOD scheme must not treat mobile phones as learning devices.

The Trust may address pupil ICT use outside school where there is a sufficient connection with the school, the conduct affects safeguarding or welfare, disrupts education, threatens another person, or damages the lawful interests of the Trust.

12. Parents, Carers and Visitors

Parents, carers, and visitors do not have access to Trust ICT facilities as a matter of course. Access may be granted for an official or visit-related purpose and will be limited to what is necessary. Users granted access must comply with this policy and may be required to sign an acceptable use agreement.

Parents and carers are expected to communicate respectfully, protect the privacy of pupils and staff, use official routes for concerns and complaints, and avoid publishing confidential or misleading information about the Trust community.

13. Data Security and Access Control

The Trust will maintain technical and organisational measures proportionate to the risks presented by its ICT environment. Access rights will follow the principle of least privilege, be reviewed periodically and be amended or removed promptly when roles change or access is no longer required.

Passwords and authentication credentials are personal and must not be shared. Users must follow current Trust password requirements, use multi-factor authentication where required and report suspected compromise immediately. Devices must be locked whenever unattended and signed out or shut down as directed.

Trust-managed devices will use appropriate security controls, supported software, security updates, firewalls, and anti-malware protection. Users must not disable or circumvent these controls. Software, browser extensions, applications, devices, and removable storage may be installed or connected only with approval.

14. Data Protection and Records Management

Personal data must be processed in accordance with the UK GDPR, Data Protection Act 2018 as amended, the Trust's Data Protection Policy and applicable privacy information. Users may access personal data only where required for an authorised purpose and must use it only for that purpose.

Trust information must be created, named, stored, shared, retained, archived, and securely disposed of under the Records Management and Retention Schedules Policy. Information must not be kept beyond an applicable retention period or deleted outside an authorised disposal process, legal hold, safeguarding requirement, or information request preservation notice.

Information rights requests and data protection complaints must be forwarded promptly to the responsible Trust contact. Users must not carry out unauthorised searches or disclosures.

15. Artificial Intelligence

Artificial intelligence may be used only where it is safe, lawful, transparent, educationally appropriate and permitted by the Trust. Human professional judgement remains responsible for decisions, communications, teaching materials, and outcomes. AI output must be checked for accuracy, bias,

appropriateness, confidentiality, intellectual property, and safeguarding risk before it is relied upon or shared.

Public or open AI tools may be used for a permitted category of work only where no personal data, pupil information, safeguarding information, confidential information, unpublished Trust material, credentials, or other identifying information is entered or uploaded.

Personal data or confidential Trust information may be processed through an AI-enabled service only where the specific product and use have been approved following safeguarding, data protection, cyber-security, procurement, and contractual assessment. Approval is not established merely because a service is described as private, enterprise or secure.

Pupil use must be authorised, supervised and age appropriate. Pupils must follow instructions about permitted assistance and acknowledgement. AI must not be used to impersonate, fabricate evidence, bully, cause harm, evade controls or make an unapproved solely automated decision about an individual.

16. Cyber Security and Incident Response

The Trust will maintain layered and current security controls including access control, supported software, appropriate patching, anti-malware protection, firewalls, multi-factor authentication, secure and resilient backups, incident response arrangements, and periodic access reviews.

The Trust will undertake cyber-risk assessment and maintain awareness, backup, and incident-response arrangements consistent with the DfE cyber-security standards. Critical systems and cloud services must be considered in continuity and recovery planning. Backup restoration and incident response will be tested at appropriate intervals.

Users must report suspicious messages, unexpected authentication prompts, payment requests, malware warnings, lost equipment, and suspected compromise without delay. Users must not respond to ransom demands or communicate with an attacker unless expressly authorised as part of incident response.

17. Internet and Wi-Fi Access

Trust wireless networks will be secured, and access allocated according to category and need. Credentials and access codes must not be shared with unauthorised individuals.

Pupil access will be filtered according to educational and safeguarding requirements. Personal pupil devices may connect only under an approved academy arrangement. Guest access may be provided where necessary for a visit or official activity and will not permit access to internal systems unless separately authorised.

18. Roles and Responsibilities

The Trust Board approves this policy and seeks assurance concerning filtering, monitoring, and cyber security. The Chief Executive Officer, CFOO, Principals and senior leaders ensure implementation, resources, and appropriate local action. The Designated Safeguarding Lead contributes to filtering and monitoring review and responds to safeguarding concerns. The DPO advises on privacy, DPIAs, data breaches and information rights. ICT support maintains approved systems and technical controls. All users must understand and comply with this policy and report concerns promptly.

19. Training, Monitoring and Review

Adult users will receive suitable induction and refresher training on acceptable use, cyber security, data protection, safeguarding, and incident reporting. Pupils will receive age-appropriate online safety education and guidance.

Implementation will be monitored by Principals, senior leaders, and ICT support. Filtering and monitoring effectiveness will be reviewed at least annually. This policy will be reviewed annually and earlier where law, statutory guidance, safeguarding risk, technology, or Trust practice materially changes. The next scheduled review is October 2028.

20. Related Policies

This policy should be read alongside the Online Safety Policy, Safeguarding and Child Protection Policy, Behaviour Policy, Data Protection Policy, Records Management and Retention Schedules Policy, Social Media Policy, Staff Code of Conduct, Personal Data Breach Procedure, mobile-phone arrangements, and relevant privacy notices.

Appendix 1: Social Media Guidance for Adult Users

Adult users should maintain clear professional boundaries and assume that material posted online may become public, be copied or be viewed out of context. Personal privacy settings reduce risk but cannot guarantee confidentiality.

Do not accept or initiate personal social media connections with pupils.
Do not discuss identifiable pupils, parents, colleagues, incidents, complaints, or confidential Trust matters.
Do not post work-related photographs, recordings or information unless authorised through an official Trust channel.
Do not use a Trust logo or present a personal account as an official account without permission.
Use multi-factor authentication where available and review privacy, location-sharing, tagging and contact-synchronisation settings.
If approached inappropriately, preserve relevant evidence, use a neutral boundary-setting response where necessary and report the matter. Do not retaliate or investigate personally.

Appendix 2: Parent and Carer Online Services Agreement

Agreement	Please tick
I will communicate respectfully and use official procedures for concerns and complaints.	☐
I will protect the privacy of pupils, staff, and other families.	☐
I will follow instructions for parent portals, learning platforms and guest access.	☐
I will keep credentials secure and report accidental access or information received in error.	☐
I will not target, threaten, harass, or unlawfully defame a member of the Trust community.	☐
I will not publish confidential information or share images or recordings of another child without an appropriate lawful basis and permission.	☐
Parent/carer name	
Name of child	
Signature	
Date	

Appendix 3: Pupil Acceptable Use Agreement

Agreement	Please tick
I will use technology only for learning or another purpose a member of staff has allowed.	☐
I will use only my own account and keep my password private.	☐
I will be kind and respectful online.	☐
I will tell a member of staff if I see or receive something harmful, worrying, or inappropriate.	☐
I will check information carefully and ask for help when unsure.	☐
I will use AI only when allowed and follow instructions about acknowledging its use.	☐
I will not bypass filtering, monitoring, or security controls.	☐
I will not bully, threaten, impersonate, or deceive anyone or create harmful or misleading content.	☐
I will not install software or connect a device without permission.	☐
I understand that Trust systems are filtered and may be monitored to help keep users and systems safe.	☐
Pupil name	
Pupil signature	
Date	
Parent/carer name	
Parent/carer signature	
Date	

Appendix 4: Adult User Acceptable Use Agreement

Agreement	Please tick
I will use Trust ICT facilities, accounts, and information only for authorised, lawful and appropriate purposes.	☐
I will maintain professional boundaries and comply with safeguarding and conduct requirements.	☐
I will protect credentials, use multi-factor authentication as required and report suspected compromise.	☐
I will use approved Trust accounts and channels and will not use personal email, messaging or cloud storage unless authorised.	☐
I will check recipients and permissions and use secure sharing methods appropriate to the information.	☐
I will access personal data only where required for my role and will follow retention and disposal requirements.	☐
I will report data breaches, security incidents, phishing, malware, lost equipment, and unauthorised disclosures immediately.	☐
I will use personal devices only where authorised and subject to Trust safeguards.	☐
I will use AI only as permitted, will not place personal or confidential information into unapproved tools, and will check outputs before use.	☐
I understand that Trust activity may be filtered, logged, monitored, reviewed, or audited lawfully and proportionately.	☐
I will cooperate with authorised investigations and preserve relevant information when instructed.	☐
Name	
Role / organisation	

Agreement	Please tick
Academy / Trust location	
Signature	
Date	

Appendix 5: Cyber Security Glossary

Term	Meaning
Anti-malware	Software designed to detect, block, and remove malicious software.
Cloud service	A service that stores, processes, or provides access to information or software over a network.
Cyber incident	An event that compromises or may compromise the confidentiality, integrity or availability of a system or information.
Encryption	Conversion of information into a protected form readable only through an authorised key or process.
Firewall	Hardware or software controlling network traffic according to security rules.
Malware	Malicious software including viruses, trojans, spyware, and ransomware.
Multi-factor authentication	Authentication using two or more different factors to verify identity.
Patching	Applying updates to correct faults or security weaknesses.
Phishing	A deceptive communication intended to obtain information, money, or unsafe action.
Ransomware	Malware that prevents access to information or systems, commonly accompanied by a payment demand.
Social engineering	Manipulating a person into disclosing information or carrying out an action that compromises security.
VPN	A virtual private network creating an encrypted connection for authorised remote access.