Every Opportunity for Every Child

Alpha Trust

Staff ICT Acceptable Use Policy

Alpha Trust Policy & Procedures No: AT P22

Committee:	Board of Trustees
Responsibility:	Trust HR
Policy reviewed:	March 2026
Approved by Alpha Trustees:	March 2026
Review cycle:	Two years, or sooner depending on statutory changes or guidance
Review due:	March 2028
Adopted by all Alpha Trust Academies	

Contents

Linked policies

- AT2 Safeguarding and Child Protection Policy
- AT P5 Discipline and Dismissal Policy
- AT P17 Staff Code of Conduct

CCHSG	A4 Behaviour, Sanctions & Rewards Policy A5 Anti-bullying Policy 44 e-Safety Policy including the Visitors Acceptable Use Policy and Cybersecurity A3 Child Protection Procedures A19 Data Protection Policy
TGS	Electronic Communications Acceptable Use Policy for Students Electronic Communications Acceptable Use Policy for Visitors Behaviour Management Policy Child Protection Policy Data Protection Policy Guidance for staff with children attending The Gilberd School
MHS	E-safety Policy Data Protection Policy Behaviour Management Policy
HFPS	E-Safety Policy (including cyber security and social media policies) Positive Behaviour Management Policy (including anti bullying) Data Protection Policy
TTS	Electronic Communications Acceptable Use Policy for Students Electronic Communications Acceptable Use Policy for Visitors Behaviour Management Policy Child Protection Policy Data Protection Policy

Legal and Regulatory Updates

This policy is reviewed and updated regularly to ensure compliance with the latest UK legislation, including the General Data Protection Regulation (GDPR), the Data Protection Act, Keeping Children Safe in Education (KCSIE) guidance, the Department for Education Meeting Digital Standards, and the National Cyber Security Center Cyber Security Standards.

Records of ICT usage, including monitoring logs and email records, are retained in accordance with the local school's data retention policy and relevant legal requirements.

Definitions

Significant Personal Use: Use of school ICT resources that exceeds incidental or minor use, as defined by HMRC.

Personal Device: Any device not owned or managed by the Trust, including mobile phones, tablets, and laptops.

Safeguarding: Measures taken to protect individuals, especially children, from harm or abuse.

Monitoring: The process of reviewing and logging ICT usage for compliance, safety, and legal purposes.

Filtering: Technical controls that restrict access to inappropriate or harmful online content.

Throughout this policy, "must" indicates a mandatory action, and "should" indicates a recommended action.

IT Equipment: Any computer, device, peripheral, software, network service, or cloud platform provided, approved, or used by the Trust or local schools for school activities.
Social media: Any online platform, app, or service used for communication, networking, or content sharing, including public, private, and group-based services. For example - Facebook, Snapchat, X, Instagram.
Official Networking Site: Any social media or online communication platform that is formally approved by the Trust or school for professional use, managed or overseen by the organisation, and used strictly for school-related communication or educational purposes.
Personal Device: Any device not owned, leased, or managed by the Trust, including mobile phones, tablets, laptops, smartwatches, and home computers.

ICT Acceptable Use Policy Overview

The Alpha Trust network of computer systems and devices is owned by the Trust and made available to staff to support their professional work. This ICT Acceptable Use Policy is written to protect all users—students, staff, and the school community. You are responsible for professional behaviour when using the systems, all resources, and the Internet. You are expected to be an active participant in e-Safety education, taking personal responsibility for yourself and your students' awareness of the opportunities and risks posed by new technologies.
This policy applies to using school resources both on-site and off-site. You agree and accept that any computer/laptop or other ICT device loaned to you by the school is provided solely to support your professional responsibilities. It is your responsibility to read the latest version of this policy because technology and the law change regularly.

Logging On and Security

- You are responsible for protecting your own network logon account and must not divulge your password to anyone.
- Do not let anyone else use your account while you are logged in. Your account is for your use only.
- Always log off or lock your screen when leaving a workstation, even for a short time.
- Respect the security settings on computers; do not attempt to bypass or alter them.
- Any attempts to access, corrupt, or destroy other user data, or compromise the privacy of others in any way, using any technology, is unacceptable.
- Computer storage areas are accessible by ICT Services Staff who may review your files, communications, and usage to ensure responsible use. This includes SharePoint Drives, User OneDrive's, Teams and networks storage areas.
- Conditional access policies may be applied to accounts to ensure security of the account, this may include Multi Factor Authentication requirements through an Authenticator app such as Microsoft Authenticator. (The organisation is unable to manage or see data on any personal device, even with the Microsoft Authenticator app installed)

Use of the Network and Computer Facilities

All users must take responsibility for their own use of new technologies, ensuring safe, responsible, and legal use.

- Whilst using any of the schools IT facilities and equipment staff should observe the following conditions:
- Report any problems with broken or damaged equipment to ICT Services immediately.

- Lost property should be handed to Reception or returned to the owner if possible.
- Staff must actively enforce the IT Acceptable Use Policy during lessons and report any serious breach to ICT Services.
- No food or drink should be consumed in any IT room.
- In the event of damage to equipment or computer malfunction, notify ICT Services by email immediately.
- When using interactive whiteboards or similar display technology, staff should freeze or pause the display to protect the privacy of any sensitive or confidential information shown.

Limited Personal Use

Incidental personal use of school equipment, networks, and email is permitted only with prior approval from your line manager.
Personal use must not interfere with school operations or your professional duties, must be reasonable in duration and frequency, and must not involve accessing or storing inappropriate material.
You must notify the school of any significant personal use.

Monitoring

All use of school internet, email, general device usage and networks is monitored and logged.
Monitoring is strictly for safeguarding and compliance purposes (e.g., legal compliance, safeguarding, suspected breaches of AUP).
There are 4 ways of monitoring available:

- Physical Monitoring - Walking around in lessons or using the relevant software for the teacher in charge to monitor what is on each screen.
- Internet and web access logs - Monitored by alerts generated by the web filter and logs generated.
- Active/Pro-active technology monitoring services - Monitored from alerts from monitoring software.
- Using Classroom Management Software - Using software solutions available to monitor student screen live within your class

Covert monitoring may be used only in exceptional circumstances, such as suspected criminal activity, and will be conducted in accordance with legal requirements.

Using IT Equipment

- Staff must ensure they know how to use equipment and explain this clearly to students.
- Students may use equipment when not under direct supervision, but it must be returned and checked by ICT Services or responsible member of staff.
- Under no circumstances should students be allowed to take equipment home or off school premises unless authorised to do so by ICT Services. (Excluding BYOD devices)
- If staff need to take equipment off-site, this must be agreed by the ICT Services. (Excluding Staff issued devices)
- Any accidental damage or equipment malfunction must be reported to ICT Services immediately.
- You have a duty to report failings in technical safeguards which may become apparent when using systems and services.

Filtering

Online filtering is used to restrict access to harmful or inappropriate websites and content categories, including discrimination, drugs, extremism, gambling, malware/hacking, pornography, piracy, self-harm, and violence. This list is indicative and not exhaustive and may change in line with technological developments and safeguarding requirements.

Staff must report any failings in technical safeguards or filtering systems.

Unacceptable Actions

- Install any unauthorised software or use online services that have not had approval. Always request this through the ICT Services Department for any programs or online services of any type on the computers.
- Damage, disable, or otherwise harm the operation of computers, or intentionally waste resources. This puts yours and others work at risk.
- Introduce a malicious code or virus. If using removable media such as USB memory sticks do not open any files that you suspect may have been infected with a virus or malicious program. The antivirus programme should notify you before infected files are opened.
- Try and gain access to an unauthorised area or system.
- Use any form of hacking or cracking software / system.
- Access, download, create, store or transmit material which is indecent or obscene, or material which could cause annoyance, offence, anxiety or distress to other network users, or material which infringes copyright, or material which is unlawful.
- Use any applications or services to bring the school or its members into disrepute.

Use of the Internet

Filtering software is used to prevent access to inappropriate internet sites and to protect computer systems. Access to the Internet is provided for school activities. Reasonable, appropriate private use is permitted in your own time, provided it does not prevent others from using resources for work purposes and is approved by your line manager. Only access appropriate material; using the Internet to obtain, download, send, print, display, or otherwise transmit or gain access to unlawful, obscene, abusive, or distressing materials is not permitted. Respect the work and ownership rights of others, including copyright laws.

Communication and Use of Email

- Conduct yourself with professionalism and respect in all forms of communication.
- School business must be conducted through official email addresses only.
- Treat email as formal written communication: content must be appropriate, accurate, and data protection compliant.
- Take extreme care with attachments from third parties.
- Do not send, receive, or forward defamatory, obscene, or otherwise inappropriate messages.
- If such an email is received, do not forward it, report immediately to ICT Services.
- School email accounts must be used for school business only.
- Personal email accounts must not be used for school business or to communicate with students.
- Emails sent on behalf of the school must be professional in language and tone.

- Email is not intended for casual communication with students or colleagues, including friendly conversation or personal matters.
- Sensitive or personal information sent externally must be password protected or encrypted, or using share links to documents.
- Use Bcc for group emails to protect privacy.
- Do not send unnecessary mass emails without consultation with the local Senior Leadership Team.
- Refer to students by initials in subject lines.
- Avoid “Reply all” unless necessary.
- Emails must not be used for routine communication with colleagues or students during teaching time unless related to safeguarding or behaviour related matters. This ensures that lessons remain focused and free from unnecessary digital distractions.
- Staff are expected to regularly delete unwanted sent and received emails from their school email accounts.
- All external emails sent on behalf of the school must include a signature containing your name, job title, and the name of the school.
- All emails are in scope of the schools mail retention period. Mailboxes, including shared mailboxes, should not be used as a storage area. Any emails required to be kept must be moved to a different location such as a network folder, or into a different solution such as SIMS. Emails that reach the set age will be automatically deleted.

Social Media

- Staff must not communicate with students or parents via personal social networking sites (e.g., Facebook).
- Professional use of social media for teaching and learning is permitted only with prior approval from senior leadership and in line with school guidelines.
- Do not accept or propose contact, nor engage in conversation with students on personal social networking sites.
- Members of staff are expected to exercise professional judgement and discretion when communicating with former students, particularly those who are under the age of 18.
- Do not discuss students, parents, colleagues, or school business on personal social networking sites.
- Do not upload pictures or videos taken in school or showing school uniform to social media sites unless authorised.
- Staff must not accept or send friend requests to current or former students under the age of 18 on personal social media accounts. A minimum interval of three years is required between the conclusion of the last professional engagement and the commencement of any personal engagement.
- Engaging with students via personal social networking platforms (such as Facebook, Instagram, Snapchat, etc.) is strictly prohibited. This helps maintain professional boundaries and protects both staff and students.
- Staff must not promote or comment on personal matters, commercial ventures, political matters, religion, or other non-school-related topics on official networking sites.

Data Protection and Security

- Ensure personal data is stored securely and used appropriately, in line with GDPR and Data Protection Act.

- Sensitive/personal information must not be stored on portable devices unless encrypted and approved by ICT Services.
- Adhere to the Cyber Security Policy to keep your account, your data and wider data and accounts safe.
- Report any accidental loss of confidential information immediately using the Incident Response Guide found in Appendix A.
- Log off or lock screens when leaving devices unattended.
- Delete or shred personal/sensitive information when no longer needed.

Copyright

The school has a Copyright Licensing Agency (CLA) Education Licence which permits:

- Works in any medium can be copied if the use is solely to illustrate a point, it is not done for commercial purposes and it is accompanied by a sufficient acknowledgement. This means minor uses, such as displaying a few lines of poetry on an interactive whiteboard, are permitted, but nothing which would undermine sales of the copied information.
- Digitally copying or photocopying from a book is limited to one full chapter or 5% of the book, whichever is greater.
- The audience of the copied works is to be teachers, students and others directly connected with the activities of the school. Copyright material cannot be used in a public document (school website, newsletters home etc.)

The Office Manager (or equivalent) must be notified of the title, source, and licensing status of any film, video, or audiovisual media intended for use in school, whether accessed via physical media, streaming services, downloads, or online platforms, and whether for educational or non-educational purposes. This requirement does not apply to short clips, extracts, or documentaries used solely for educational purposes and covered by the school's existing licences.

Device and Data Security (Including Cloud Storage)

School data must only be stored or shared using cloud storage providers that have been authorised by the Trust or your school's ICT Services. The use of unauthorised third-party cloud services for school data is not permitted.

Organisational data (including student names, personal details, or any sensitive information) must only be stored on school-owned, encrypted devices or approved cloud services. Storing such data on personal devices (including home desktops, laptops, tablets, or phones) is strictly prohibited. An exception to this is organisational emails being access on personal phones via apps. This is controlled and managed by organisational technical policies to ensure encryption and data security.

Use of Personal Devices

- Personal devices may only be used in school with explicit permission from senior leadership or ICT services.
- Personal mobiles must be secured, not accessible to students, and used only during authorised breaks.
- Do not use personal devices to call, text, email, or message students, or divulge personal contact details.
- Do not connect personal devices to the school network without explicit permission and adequate virus protection. (Or use the Authenticated Wireless if available)

- No pictures or videos may be taken within school or at school activities on personal devices.

Remote/Online Learning and Video Conferencing

- Safeguarding principles should be applied to every online learning platform, virtual classroom, or digital learning environment where students interact with each other, staff or external agencies whenever possible. To ensure appropriate oversight, examples include holding meetings in an open area on site, recording sessions, or inviting another staff member to join the team or meeting.
- Parental permission is required for student participation in live streams.
- Clear ground rules must be established and reiterated.
- Students must not record, reproduce, or redistribute materials from live streams.
- All participants should be in neutral areas (not bedrooms/bathrooms).
- Personal information must not be disclosed.
- School email addresses only; usernames/passwords must not be shared.
- Audio participation or live chat is acceptable; video is optional but should be used where possible.
- Dress code must be appropriate.
- No one-to-one remote learning between staff and students unless authorised and recorded.
- Recordings must be stored securely and only shared when necessary.
- Staff must use appropriate backgrounds or blur features if on camera.

ICT Services

- Any problems or faulty equipment must be reported to the ICT Services Helpdesk immediately.
- Staff and students should not attempt to repair equipment themselves.
- ICT Services will manage device encryption. No user other than ICT Services staff may decrypt drives, either temporarily or permanently.
- All laptops, memory sticks, and portable devices used for school business must be encrypted to protect sensitive information.
- For staff who access school email through mobile phones, ICT Services reserves the right to remotely wipe the device of organisational data if it is lost or stolen, to prevent data breaches.
- Failure to notify ICT Services of a lost or stolen device may result in personal liability for any data breach or fines incurred.
- All corporate-owned devices are filtered and monitored to comply with safeguarding requirements.
- ICT Services will restrict access to accounts and data when login methods are considered insecure or present a significant security risk.
- Personal mobile devices are permitted to access the BYOD Network (Authenticated Wireless). Either you or ICT Services staff must install the Filtering Certificate on your device to be able to connect when on site.
- ICT Services will conduct periodic asset checks to confirm devices assigned to users still match records to ensure asset management accuracy. This may require you to bring the device to ICT Services for this check.
- Any device issued will need to be returned to ICT Services at the end of contract.

Training & Awareness

Annual cyber security and GDPR training is required each year to keep knowledge and understanding aligned with the latest trends and legal requirements.

Training needs identified by staff may be submitted to ICT Services IT Helpdesk for review and potential implementation. Support and training can be provided in various formats, such as video guides, written documentation, or one-to-one guidance sessions.

Periodic phishing test emails are sent to ensure staff keep alert to any potential suspicious activity or attack. Staff should follow local policies in relation to reporting these types of emails.

External Messaging Groups

While staff may choose to join informal messaging groups outside the organisation, we do **not recommend** this for several reasons:

- **Professional Boundaries**: Informal groups can blur the line between personal and professional relationships, leading to misunderstandings or conflicts.
- **Safeguarding Concerns**: Conversations in unmonitored spaces cannot be reviewed or audited, which may create safeguarding risks.
- **Reputational Risk**: Comments made in private groups can be shared publicly, potentially harming individual or organisational reputation.
- **Wellbeing & Inclusion**: Gossip or exclusionary behaviour in private groups can negatively impact workplace culture and staff wellbeing.

Disciplinary Procedures

Breaches of this policy may result in withdrawal of access, disciplinary action, and/or legal proceedings. Where appropriate, police or other authorities may be involved.

e-Safety

Further advice on all e-Safety issues can be found at; www.ceop.gov.uk , www.thinkuknow.co.uk , www.childnet.com

Please read this document carefully. Only once it has been signed and returned will access to the school computer network be permitted.

I have read and understood the above and agree to uphold the standards outlined within these guidelines.

Staff Name: _____

Signature: _____ Date: _____

Appendix A – Incident Response Guide

This guide must be followed **immediately** if you suspect a data breach, cyber security incident, loss of equipment, or loss or unauthorised disclosure of confidential information.

1. Immediate Actions

- If you know how to do so, immediately disconnect the affected device from the network (for example by turning off Wi-Fi or unplugging the network cable).
- If you are unsure how to disconnect the device from the network, or are uncertain what action to take, power off the device immediately.
- Secure the device and do not allow others to use it.

2. Reporting the Incident

- Report the incident as soon as possible to:
    - Your school's Data Protection Officer (DPO), and
    - ICT Services
- Provide clear and accurate information, including:
    - What has happened
    - When it was discovered
    - The type of device, system, or data involved
    - Any actions already taken

3. What Not to Do

- Do not attempt to investigate, repair, or resolve the issue yourself.
- Do not delete, alter, or move files, emails, messages, or logs related to the incident.
- Do not discuss the incident with colleagues, students, parents, or external parties unless authorised.

4. Follow-up Actions

- Follow all instructions provided by the DPO or ICT Services.
- Cooperate fully with any investigation, containment, or reporting requirements.
- Further action may be required to meet data protection, safeguarding, or legal obligations.

Failure to report incidents promptly may increase safeguarding and legal risks and may result in disciplinary action.