Staff IT and Electronic Devices Policy

Date adopted: September 2026

Review Period: 1 year

Next review: September 2027

History of most recent policy reviews

Date (Annual)	Review	Governor Committee with responsibility
25th September 2023	Annual	Education
September 2024	Annual	Education
September 2025	Annual	Education
September 2026	Annual	Education

Contents:

Statement of intent

1. Legal framework
2. Roles and responsibilities
3. Classifications
4. Acceptable use
5. Emails and the internet
6. Portable equipment
7. Personal devices
8. Removeable media
9. Cloud-based storage
10. Storing messages
11. Unauthorised use
12. Loaning electronic devices
13. Purchasing
14. Safety and security
15. Loss, theft and damage
16. Implementation
17. Monitoring and review

Statement of intent

Air Balloon Hill Primary School believes that IT plays an important part in both teaching and learning over a range of subjects, and the school accepts that both school-owned and personal electronic devices are widely used by members of staff. The school is committed to ensuring that both staff and pupils have access to the necessary facilities and support to allow them to carry out their work.

The school has a sensible and practical approach that acknowledges the use of devices, and this policy is intended to ensure that:

- Members of staff are responsible users and remain safe while using the internet.
- School IT systems and users are protected from accidental or deliberate misuse which could put the security of the systems and/or users at risk.
- Members of staff are protected from potential risks in their everyday use of electronic devices.
- A process is in place for claiming financial payments when electronic devices are lost or damaged by members of staff.

Personal use of IT equipment and personal devices is permitted at the school; however, this is strictly regulated and must be done in accordance with this policy, the Staff Code of Conduct and the Online Safety and Social Media Policy.

1. Legal framework

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- Online Safety Act 2023
- Data Protection Act 2018
- Computer Misuse Act 1990
- Communications Act 2003
- Freedom of Information Act 2000
- Human Rights Act 1998
- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)

This policy operates in conjunction with the following school policies:

- Data Protection Policy
- Freedom of Information Policy
- Complaints Procedures Policy
- Disciplinary Policy and Procedure
- Online Safety Policy
- Data Protection Impact Assessment Policy & Procedure
- Finance Policy
- Records Management Policy

2. Roles and responsibilities

The governing body has the responsibility for the overall implementation of this policy, ensuring it remains compliant with relevant legislation.

The headteacher is responsible for:

- Reviewing and amending this policy with the DSL, taking into account new legislation, government guidance and previously reported incidents, to improve procedures.
- The day-to-day implementation and management of the policy.
- The overall allocation and provision of resources.
- Handling complaints regarding this policy as outlined in the school's Complaints Procedures Policy.
- Informing staff that the school reserves the right to access personal devices for the purpose of ensuring the effectiveness of this policy.

The IT Support Service is responsible for:

- Carrying out checks on internet activity of user accounts if and when required by the headteacher.
- Remotely viewing or interacting with any of the computers on the school's network. This may be done randomly to implement this policy and to assist in any difficulties.

- Ensuring routine security checks are carried out on all school-owned devices that are used for work purposes to check that appropriate security measures and software have been updated and installed.
- Ensuring that, though appropriate steps will be taken to ensure personal information is not seen during security checks, staff are made aware of the potential risks.
- Accessing files and data to solve problems for a user, with their authorisation.
- Adjusting access rights and security privileges in the interest of the protection of the school's data, information, network and computers. in conjunction with the School Business Manager.
- Disabling user accounts of staff who do not follow this policy, at the request of the headteacher. In conjunction with the School Business Manager.
- Assisting the headteacher in all matters requiring reconfiguration of security and access rights and in all matters relating to this policy. in conjunction with the School Business Manager.
- Assisting staff with authorised use of the IT facilities and devices, if required.
- Immediately reporting any breach of personal devices to the School Business Manager.
- Ensuring that all school-owned and personal electronic devices have security software installed, to protect sensitive data in cases of loss or theft.
- The maintenance and day-to-day management of the equipment, as well as the device loans process, in conjunction with the School Business Manager.

The School Business Manager is responsible for:

- Reporting any breaches of the Data Protection Policy to the appropriate authorities.
- Ensuring all staff are aware of, and comply with, the data protection principles outlined in the school's Data Protection Policy.
- Maintaining a Fixed Asset Register to record and monitor the school's assets.
- Ensuring value for money is secured when purchasing electronic devices.
- Monitoring purchases made under the Finance Policy.
- Overseeing purchase requests for electronic devices.

Staff members are responsible for:

- Requesting permission from the headteacher, subject to their approval, before using school-owned devices for personal reasons during school hours.
- Requesting permission to loan school equipment and devices from the headteacher or School Business Manager.
- Ensuring any personal devices that are connected to the school network are encrypted in a manner approved by the IT Support Service
- Reporting misuse of IT facilities or devices, by staff or pupils, to the headteacher.

- Reading and signing a Device User Agreement to confirm they understand their responsibilities and what is expected of them when they use school-owned and personal devices.

3. Classifications

School-owned and personal devices or IT facilities include, but are not limited to, the following:

- Computers, laptops and software
- Monitors
- Keyboards
- Mouses
- Scanners
- Cameras
- Other devices including furnishings and fittings used with them
- Mail systems (internal and external)
- Internet and intranet (email, web access and video conferencing)
- Telephones (fixed and mobile)
- Tablets and other portable devices
- Computers
- Photocopying, printing and reproduction equipment
- Recording and playback equipment
- Documents and publications (any type of format)

4. Acceptable use

This policy applies to any computer or other device connected to the school's network and computers.

The school will monitor the use of all IT facilities and electronic devices. Members of staff will only use school-owned and approved personal devices for work duties and educational purposes. The duties for which use is permitted include, but are not limited to, the following:

- Preparing work for lessons, activities, meetings, reviews, etc.
- Researching any school-related task
- Any school encouraged tuition or educational use
- Collating or processing information for school business
- Communicating with other members of staff, such as contacting the school office for assistance

Inappropriate use of school-owned and personal devices could result in a breach of the school's Data Protection Policy.

Inappropriate use of school-owned and personal devices could result in a breach of legislation, including the UK GDPR and Data Protection Act 2018.

Any member of staff found to have breached the school's Data Protection Policy or relevant legislation will face disciplinary action.

Staff will always be an example of good practice to pupils, serving as a positive role model in the use of IT and related equipment.

Since IT facilities are also used by pupils, the school will have acceptable use agreements in place for pupils – staff will ensure that pupils comply with these.

Pupils found to have been misusing the IT facilities will be reported to the IT Manager and subsequently to the Headteacher if deemed to be serious.

School-owned electronic devices will not be used to access any material which is illegal, inappropriate, or may cause harm or distress to others.

Any illegal, inappropriate or harmful activity will be immediately reported to the headteacher.

Members of staff will not:

- Open email attachments from unknown sources. Anything suspicious should be forwarded to the IT Manager for investigation.
- Use programmes or software that may allow them to bypass the filtering or security systems.
- Upload or download large capacity files (over 500MB) without permission from the IT Manager.
- Give their home address, phone number, social networking details or email addresses to pupils or parents – contact with parents will be done through authorised school contact channels.

All data will be stored appropriately in accordance with the school's Data Protection Policy.

Members of staff will only use school-owned electronic devices to take pictures or videos of people who have given their consent.

School-owned electronic devices will not be used to access personal social media accounts.

Personal electronic devices will not be used to communicate with pupils or parents, including via social media except where a declaration form has been completed in line with the School's Code of Conduct.

Staff will ensure they:

- Express neutral opinions when representing the school online.
- Avoid disclosing any confidential information or comments regarding the school, or any information that may affect its reputability.
- Have the necessary privacy settings applied to any social networking sites.

Images or videos of pupils, staff or parents will only be published online for the activities which consent has been sought.

Copyrighted material will not be downloaded or distributed.

School-owned devices can be taken home for work purposes only, once approval has been sought from the headteacher and IT Manager. Remote access to the school network will be given to staff using these devices at home.

School equipment that is used outside the premises, e.g. laptops, will be returned to the school when the employee leaves employment, or if requested to do so by the headteacher.

While there is scope for staff to utilise school equipment for personal reasons, this will not be done during working hours unless approved by the headteacher or in the case of a personal emergency.

Private business will not be mixed with official duties, e.g. work email addresses will be reserved strictly for work-based contacts only.

Use of a school-owned phone for personal use will be permitted for necessary calls.

Personal use of school-owned equipment can be denied by the headteacher at any time. This will typically be because of improper use or over-use of school facilities for personal reasons. A charge may be made for using equipment if the values are significant.

Where permission has been given to use the school equipment for personal reasons, this use will take place during the employee's own time, e.g. during lunchtime or after school. Where this is not possible, or in the case of an emergency, equipment can be used for personal reasons during work hours provided that disruption to the staff member's work, and the work of others, is minimal.

Abuse of IT facilities or devices could result in privileges being removed. Staff will be aware of acceptable IT use, and misuse of the facilities, as defined in this policy, will be reported to the headteacher.

Failure to adhere to the rules described in this policy may result in disciplinary action, in line with the Disciplinary Policy and Procedure.

5. Emails and the internet

The school email system and internet connection are available for communication and use on matters directly concerned with school business.

Unprofessional messages will not be tolerated. All emails will be written in a professional tone and will be proofread by the staff member sending the email, to ensure this prior to sending.

Abusive messages will not be tolerated – any instant of abuse may result in disciplinary action.

If any email contains confidential information, the user will ensure that the necessary steps are taken to protect confidentiality.

The school will be liable for any defamatory information circulated either within the school or to external contacts. Any instances brought to the attention of the school will be investigated.

The school email system and accounts will never be registered or subscribed to spam or other non-work-related updates, advertisements or other personal communications. School email addresses will not be shared without confirming that they will not be subjected to spam or sold on to marketing companies.

All emails that are sent or received will be retained within the school in line with the school Records Management Policy. The timeframe will be altered where an inbox becomes full.

All emails being sent to external recipients will contain the school standard confidentiality notice. That notice will normally be configured as a signature by the IT Support Service and will not be removed.

Staff linking work email accounts to personal devices, subject to the headteacher's approval, will sign the Device User Agreement and submit their devices for security checks when requested.

Contracts sent via email or the internet are as legally binding as those sent on paper. An exchange of emails can lead to a contract being formed between the sender, or the school, and the recipient. Staff will never commit the school to any obligations by email or the internet without ensuring that they have the authority to do so.

Purchases for school equipment will only be permitted to be made online with the permission of the headteacher, and a receipt will be obtained in order to comply with monitoring and accountability. Hard copies of the purchase will be made for the purchaser and the SBM. This is in addition to any purchasing arrangement followed according to the school's Finance Policy.

6. Portable equipment

All data on school-owned equipment will be synchronised with the school server and backed up regularly.

Portable equipment will be transported in its protective case, if supplied.

Where the school provides mobile technologies, such as phones, laptops and personal digital assistants, for off-site visits and trips, staff will only use these devices.

7. Personal devices

Staff members will use personal devices in line with the school's Staff Code of Conduct, Online Safety and Social Media Policy and Data Protection Impact Assessment Policy & Procedure.

All personal devices that are used to access the school's online portal, systems or email accounts, e.g. laptops or mobile phones, will be declared and approved by the headteacher before use and submitted for the routine checks outlined in section 14 of this policy.

Approved devices will be secured with a password or biometric access control, e.g. fingerprint scanner.

Personal devices will only be used for off-site educational purposes e.g. to contact the school in an emergency, when no other school issued device is available.

Inappropriate messages will not be sent to any member of the school community.

Permission will be sought from the owner of a device before any image or sound recordings are made on their personal device. Consent will also be obtained from staff, pupils and other visitors if photographs or recordings are to be taken.

Members of staff bringing personal devices into school will ensure that there is not any inappropriate or illegal content on their device.

Staff members and visitors are not permitted to use personal mobile devices, smartwatches, or other recording-capable wearable technology during lesson time, during supervision duties, or in the presence of pupils, except in an emergency or when specifically authorized by the Headteacher. Personal devices must be kept on silent and stored out of sight or pupils. Under no circumstances may personal devices be used to photograph, record, or communicate with pupils, nor should they be handed to pupils.

8. Removable media

Only recommended removable media will be used including, but not limited to, the following:

- DVDs
- CDs

No personal USB devices to be used without the prior permission of the Headteacher.

9. Cloud-based storage

Data held in remote and cloud-based storage is still required to be protected in line with the UK GDPR and DPA 2018; therefore, members of staff will ensure that cloud-based data is kept confidential and no data is copied, removed or adapted

10. Storing messages

Information and data on the school's network and computers will be kept in an organised manner and should be placed in a location of an appropriate security level.

If a member of staff is unsure about the correct message storage procedure, help will be sought from the IT Support Service.

Employees who feel that they have cause for complaint as a result of any communications on school-owned devices will raise the matter initially with the Headteacher, as appropriate. The complaint will then be raised through the grievance procedure in line with the Grievance Policy.

11. Unauthorised use

Staff will not be permitted, under any circumstances, to:

- Use the IT facilities for commercial or financial gain without the explicit written authorisation from the headteacher.
- Physically damage IT and communication facilities or school-owned devices.
- Relocate, take off-site, or otherwise interfere with the IT facilities without the authorisation of the School Business Manager or headteacher.

- Use or attempt to use someone else's user account. Users will create strong passwords or passphrases in line with NCSC guidance. Passwords will not be routinely changed on a fixed schedule unless a breach or compromise is suspected. Multi-Factor Authentication (MFA) must be enabled for all remote access to school systems and email. User account passwords must never be shared or disclosed. Use the IT facilities at any time to access, download, send, receive, view or display any of the following:
    - Any material that is illegal
    - Any message that could constitute bullying, harassment (including on the grounds of sex, race, religion/religious belief, sexual orientation or disability) or any negative comment about other persons or organisations
    - Online gambling
    - Remarks, which may adversely affect the reputation of any organisation or person, whether or not you know them to be true or false
    - Any sexually explicit content, or adult or chat-line phone numbers
- Generate messages or documents that appear to originate from someone else or otherwise impersonate someone else.
- Install hardware or software without the consent of the School Business Manager or the headteacher.
- Introduce any form of stand-alone software or removable hardware likely to cause malfunctioning of the IT facilities or that will bypass, over-ride or overwrite the security parameters on the network or any of the school's computers.
- Use or attempt to use the school's IT facilities to undertake any form of piracy, including the infringement of software licenses or other copyright provisions whether knowingly or not. This is illegal.
- Purchase any IT facilities without the consent of the School Business Manager or headteacher. This is in addition to any purchasing arrangements followed according to the Finance Policy.
- Use or attempt to use the school's phone lines for internet or email access unless given authorisation by the headteacher. This will include using or attempting to use any other form of hardware capable of telecommunication, regardless of ownership.
- Use any chatlines, bulletin boards or pay-to-view sites on the internet. In addition, staff will not download or attempt to download any software of this nature.
- Use the internet for any auctioning activity or to purchase items unless given authority to do so by the headteacher. This is in addition to any purchasing arrangement followed according to the Finance Policy.
- Knowingly distribute or introduce a virus or harmful code onto the school's network or computers. Doing so may result in disciplinary action, including summary dismissal.
- Copy, download or distribute any material from the internet or email that may be illegal to do so. This can include computer software, music, text, and video clips. If a staff member it is not clear that they have permission to do so, or if the permission cannot be obtained, they will not download the material.
- Use, or attempt to use, the communication facilities to call overseas without the authorisation of the headteacher.
- Obtain and post on the internet, or send via e-mail, any confidential information about other employees, the school, its customers or suppliers.
- Interfere with someone else's use of the IT facilities.
- Be wasteful of IT resources, particularly printer ink, toner and paper.

- Use the IT facilities when it will interfere with their responsibilities to supervise pupils.
- Share any information or data pertaining to other staff or pupils at the school with unauthorised parties. Data will only be shared for relevant processing purposes.
- Operate equipment to record an image beneath a person's clothing with the intention of observing, or enabling another person to observe, the victim's genitals or buttocks without their knowledge or consent, whether exposed or covered by underwear – otherwise known as "upskirting".

Any unauthorised use of email or the internet will likely result in disciplinary action, including summary dismissal, in line with the Disciplinary Policy and Procedure.

If a member of staff is subjected to, or knows about harassment, upskirting or bullying that has occurred via staff email or through the use of school-owned devices, they will report this immediately to the headteacher.

12. Loaning electronic devices

School equipment, including electronic devices, will be loaned to staff members in agreement with the Headteacher and the School Business Manager.

Loans will be requested using the loan request form and must give at least three working days' notice prior to the requested loan date.

Equipment and devices will only be loaned to staff members who have read, signed and returned the terms of use, as set out in the staff declaration form.

By loaning school equipment and electronic devices, staff members will be agreeing to act in accordance with the terms of acceptable use.

Once a request has been authorised, the staff member will be required to undergo any training required to use the requested equipment, including how to store, handle and undertake any maintenance, e.g. changing batteries.

The maximum loan period to be agreed when requesting the loan of equipment.

If the equipment or device is no longer required, staff members will return the equipment to the School Business Manager as soon as possible, allowing the equipment to be made available to someone else.

Devices allowed for loan will be password protected to ensure the security of any data they hold.

13. Purchasing

Requests for equipment or electronic devices will be processed in line with the school's purchasing procedures.

Requests will be submitted in sufficient detail for an informed decision to be made.

Individual staff members will not be permitted to purchase equipment or devices, or process payments for such goods, on the school's behalf unless permission has been sought from the headteacher.

The cost of any equipment or devices personally purchased by staff members will not be reimbursed by the school, unless otherwise specified by the headteacher.

The SBM will seek advice from the IT Support Service and professionals when purchasing equipment.

All equipment and electronic devices will be sourced from a reputable supplier.

The SBM will maintain a Fixed Asset Register which will be used to record and monitor the school's assets. All equipment and electronic devices purchased using school funds will be added to this register.

When devices are not fit for purpose, staff members may request new equipment. If their request is granted, the old equipment or electronic device will be returned to the School Business Manager, including any accessories which were originally included with the device. Any old devices will then be disposed of or wiped clear by the IT Support Service.

14. Safety and security

The school's network will be secured using firewalls in line with the Data Protection Impact Assessment Policy & Procedure.

Filtering of websites, as detailed in the Data Protection Impact Assessment Policy & Procedure, will ensure that access to websites with known malware are blocked immediately and reported to the School Business Manager, who will inform the Local Authority.

The school operates robust web filtering and monitoring systems in compliance with DfE Standards and Keeping Children Safe in Education (KCSIE). The IT Support Service, in conjunction with the School Business Manager and Designated Safeguarding Lead (DSL) regularly reviews filtering block lists, system alerts, and user logs. Any attempts to access blocked, harmful, or inappropriate material will be logged, automatically alerted to the DSL/Headteacher, and investigated immediately.

Approved anti-virus software and malware protection will be used on all approved devices and will be updated regularly.

The school will use mail security technology to detect and block any malware transmitted via email – this will be reviewed regularly.

Members of staff will ensure that all school-owned electronic devices are made available for anti-virus updates, malware protection updates and software installations, patches or upgrades, on a regular basis.

Where it is agreed for personal devices to be used for school purposes, it is the responsibility of the member of staff to ensure that the device is kept up to date with both anti-virus and computer updates.

Programmes and software will not be installed on school-owned electronic devices without permission from the IT Support Service.

Staff will not be permitted to remove any software from a school-owned electronic device without permission from the IT Support Service.

Members of staff who install or remove software from a school-owned electronic device without seeking authorisation, may be subject to disciplinary measures.

All devices will be secured by a password or biometric access control.

Passwords will be kept confidential and must not be shared with pupils, unauthorised members of staff or third parties.

Devices will be configured so that they are automatically locked after being left idle for a set time.

Further security arrangements are outlined in the Data Protection Impact Assessment Policy & Procedure.

15. Loss, theft and damage

For the purpose of this policy, **"damage"** is defined as any fault in a school-owned electronic device caused by the following:

- Connections with other devices, e.g. connecting to printers which are not approved by the IT Support Service
- Unreasonable use of force
- Abuse
- Neglect
- Alterations
- Improper installation

The school's insurance may cover school-owned electronic devices that are damaged or lost.

Staff members will use school-owned electronic devices within the parameters of the school's insurance cover – if a school-owned electronic device is damaged or lost outside of school hours and/or off-site, the member of staff at fault may be responsible for paying damages.

Any incident that leads to a school-owned electronic device being lost will be treated in the same way as damage.

The IT Support Service and headteacher will decide whether a device has been damaged due to the actions described above.

The IT Support Service will be contacted if a school-owned electronic device has a technical fault.

If a school-owned or approved personal device containing or accessing school data is lost, stolen, or compromised, the staff member must report the incident immediately to the School

Business Manager and IT Support Service. This will enable remote wiping of data and allow the Data Protection Officer (DPO) to assess whether a personal data breach report to the Information Commissioner's Office (ICO) is required.

The school will not be responsible for the loss, damage or theft of any personal device, including phones, cameras, tablets, smart watches, removable media, etc. whilst on school premises.

16. Implementation

Staff will report any breach of this policy to the headteacher.

The IT Support Service may remotely view or interact with any of the computers on the school's network. This may be used randomly to implement this policy and to assist in any difficulties.

The school's network has anti-virus software installed.

Attempting to access the school's systems using another employee's user account and/or password without prior authorisation will likely result in disciplinary action, including summary dismissal.

User accounts will be accessible by the IT Support Service when necessary.

Users will ensure that critical information is not stored solely within the school's computer system. Where appropriate, critical information is stored on secure cloud-based systems.

Users will be required to familiarise themselves with the requirements of the UK GDPR and Data Protection Act 2018, and to ensure that they operate in accordance with the requirements of the regulations and the Data Protection Policy.

Any breach of the rules in this policy may result in disciplinary action, which may lead to dismissal.

A misuse or breach of this policy could also result in criminal or civil actions being brought against the persons involved or the school.

17. Monitoring and review

This policy will be reviewed annually by the Designated Safeguarding Lead.

Any changes or amendments to this policy will be communicated to all staff members.

The scheduled review date for this policy will be September 2027