



Staff ICT and Electronic Devices Policy

Strive for Education

Approved by:	S Brown	Creation Date:	June 2025 (<i>Replaces ICT Acceptable Use and Social Media Policy</i>)
Last reviewed on:		Next review date:	June 2027
Location:	SharePoint: Staff Area > Staff Information > Policies Website: https://striveforeducation.co.uk/policies/ iHasco – Linked to Safeguarding Training module		

Changes since last review:

New and updated information in this policy is highlighted in **[blue filled and bold text]**.

Contents:

Statement of intent

1. [Legal framework](#)
2. [Roles and responsibilities](#)
3. [Classifications](#)
4. [Acceptable use](#)
5. [Emails and the internet](#)
6. **[Updated]** [Portable equipment](#)
7. **[Updated]** [Personal devices](#)
8. **[Updated]** [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](#)

Appendices

- A. [Staff Declaration](#)

Statement of intent

Strive for Education (Strive) believes that ICT 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 students 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 ICT 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.
- Staff do not use their own personal computers connected to the Strive network.

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

1. Legal framework

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

- 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
- Photography and Images Policy
- Data and Cyber-security Breach Prevention and Management Plan
- Records Management Policy

2. Roles and responsibilities

The proprietors have 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 Operations Director. The Operations Director acts as the Data Protection Officer (DPO), taking into account new legislation, government guidance and previously reported incidents, to improve procedures.
- 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 Operations Director is responsible for:

- The day-to-day implementation and management of the policy.
- The overall allocation and provision of resources.
- Managing the Filtering and Monitoring systems which are in place to secure the internet activity of all user accounts and to report any inappropriate use to the Headteacher.

- In conjunction with the external IT supplier ensuring that all school-owned devices have security software installed, to protect sensitive data in cases of loss or theft.
- Ensuring that all school-owned devices are secured and encrypted in line with the school's Data Protection Policy.
- Ensuring that all devices connected to the school network and internet are encrypted.
- Ensuring all staff are aware of, and comply with, the data protection principles outlined in the school's Data Protection Policy.

External IT supplier

- Remotely viewing or interacting with any of the computers on the school's network. This is only done via an organised session and is not done without prior consent. Staff will be sent an invitation to download and run the remote access software, this has to be initiated by the staff member.
- 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.
- Disabling user accounts of staff who do not follow this policy, at the request of the Headteacher/ Operations Director.
- Assisting the Headteacher in all matters requiring reconfiguration of security and access rights and in all matters relating to this policy.
- Assisting staff with authorised use of the ICT facilities and devices, if required.
- Immediately reporting any breach of personal devices to the Operations Director.
- Maintaining a Fixed Asset Register to record and monitor the school's assets.

Staff members are responsible for:

- Requesting permission from the Headteacher or Operations Director, 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.
- Ensuring any personal devices that are not connected to the school network.
- Reporting misuse of ICT facilities or devices, by staff or students, 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 ICT facilities include, but are not limited to, the following:

- Computers, laptops and software

- Monitors
- Keyboards
- Mouses
- Scanners
- Cameras
- Camcorders
- 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 ICT facilities and electronic devices. Members of staff will only use school-owned 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 devices could result in a breach of the school's Data Protection Policy.

Inappropriate use of school-owned 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 students, serving as a positive role model in the use of ICT and related equipment.

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

Students found to have been misusing the ICT facilities will be reported to the Headteacher.

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.
- Use programmes or software that may allow them to bypass the filtering or security systems.
- Upload or download extra-large capacity files without permission from the external IT supplier.
- Give their home address, phone number, social networking details or email addresses to students 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. An update list of students and staff who have consented can be found in [Staff Area > Staff Information > Photography consent](#) this is also noted in student Arbor records.

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

Personal electronic devices will not be used to communicate with students or parents, including via social media.

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 students, staff or parents will only be published online for the activities which consent has been sought.

Copyrighted material will not be downloaded or distributed.

Permission is granted for school-owned devices to be taken home for work purposes. Secure 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 emergency or 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.

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

More details about acceptable use can be found in the staff Technology Acceptable Use Agreement and Device User Agreement.

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.

Emails will not be used as a substitute for face-to-face communication, unless it is otherwise impossible.

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.

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 for a period of 12 months by default. More information can be found in the 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.

Personal email accounts will only be accessed via school computers outside of work hours and only if they have built-in anti-virus protection approved by the external IT supplier. Staff will ensure that access to personal emails never interferes with work duties.

Staff linking work email accounts to personal devices, subject to the Headteacher's approval.

The types of information sent through emails to a personal device will be limited to ensure the protection of personal data, e.g. students' details.

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 or Operations Director, and a receipt will be obtained in order to comply with monitoring and accountability.

Any suspicious emails will be recorded in the incident log and will be reported to the Operations Director. All incidents will be responded to in accordance with the Online Safety Policy.

6. [Updated] Portable equipment

All data on school-owned equipment will be backed up automatically three times a day, OneDrive, SharePoint and Teams, individual Desktop files are not backed up, staff are encouraged to save files into areas on SharePoint in order to ensure that files are backed up.

Portable school-owned electronic devices will not be left unattended, and instead will be kept out of sight and securely locked away when they are not in use.

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

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

7. [Updated] Personal devices

Staff members do not use personal devices to access the school's online SharePoint, systems or email accounts.

8. [Updated] Removable media

Removable media such as USB drives, can only be used where express permission is granted by the external IT supplier.

In no circumstances will personal and confidential information be stored on any removable media.

Removable media will be disposed of securely by the external IT supplier at the request of the Operations Director.

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

Emails and messages stored on school-owned devices will be stored digitally or in a suitable hard copy file and disposed of after no more than six months.

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

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 Operations Director, 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 ICT facilities for commercial or financial gain without the explicit written authorisation from the Headteacher.
- Physically damage ICT and communication facilities or school-owned devices.
- Relocate, take off-site, or otherwise interfere with the ICT facilities without the authorisation of the Operations Director or Headteacher. Certain items are asset registered, and security marked; their location is recorded by the external IT supplier and the Operations Director for accountability. Once items are moved after authorisation, staff will be responsible for notifying the Operations Director of the new location.
- Use or attempt to use someone else's user account. All users of the ICT facilities will be issued with a unique user account and password. User account passwords will never be disclosed to or by anyone.
- Use the ICT 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 or attempt to install hardware or software without the consent of the external IT supplier or the Operations Director.

- Introduce any form of stand-alone software or removable hardware likely to cause malfunctioning of the ICT 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 ICT 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 ICT facilities without the consent of the Operations Director or Headteacher.
- Use any chat-lines, 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.
- 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.
- Use the ICT facilities for personal use without the authorisation of the Headteacher. This authorisation will be requested on each occasion of personal use.
- 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 ICT facilities.
- Be wasteful of ICT resources, particularly printer ink, toner and paper. Printing should be in black and white by default with colour printing only being used where absolutely necessary.
- Use the ICT facilities when it will interfere with their responsibilities to supervise students.
- Share any information or data pertaining to other staff or students 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.Purchasing

Funding for electronic devices will be budgeted and predetermined by the proprietors.

Requests for equipment or electronic devices will be made in writing to the Headteacher or Operations Director. Requests will be submitted in sufficient detail for an informed decision to be made.

Requests will be responded to within three working days. If sufficient detail is not provided, the request will not be processed.

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.

In relation to devices for a specific project, project budget holders will provide evidence and a written statement requesting the necessary funds for the equipment required.

The Operations Director will seek advice from the external IT supplier and professionals when purchasing equipment.

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

The Operations Director 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, or are at least four years old, staff members may request new equipment. If their request is granted, the old equipment or electronic device will be returned to the Operations Director, including any accessories which were originally included with the device. Any old devices will then be disposed of or wiped clear by the external IT supplier.

13.Safety and security

The school's network will be secured using firewalls.

Filtering of websites, will ensure that access to websites with known malware are blocked immediately and reported to the external IT supplier.

Approved anti-virus software and malware protection will be used on all approved devices and will be updated by the external IT supplier.

The school will use mail security technology to detect and block any malware transmitted via email.

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. Staff will ensure to adhere to any messages regarding updates given by the computer, they will also ensure that a full shut down and re-start is performed regularly, at least once a week.

Programmes and software will not be installed on school-owned electronic devices without permission from the Operations Director.

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

Members of staff who install or remove software from a school-owned electronic device without seeking authorisation from the Operations Director, 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 students, 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. This will be no more than 3 minutes for desktop computers or laptops.

All devices must be encrypted using a method approved by the DPO with advice from the external IT supplier.

14.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 external IT supplier
- Unreasonable use of force
- Abuse
- Neglect
- Alterations
- Improper installation

The school’s insurance will cover school-owned electronic devices that are damaged or lost, during school hours, if they are being used on the school premises.

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 Headteacher and Operations Director will decide whether a device has been damaged due to the actions described above.

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

If it is decided that a member of staff is liable for the damage, they will be required to pay 20 percent of the total repair or replacement cost. A written request for payment will be submitted to the member of staff who is liable to pay for damages.

If the member of staff believes that the request is unfair, they can make an appeal to the Headteacher, who will make a final decision within two weeks.

In cases where the Headteacher decides that it is fair to seek payment for damages, the member of staff will be required to make the payment within six weeks of receiving the request.

Payments will be made to the Operations Director via the main office, and a receipt is given to the member of staff.

The school will accept payments made via bank transfer.

A record of the payment will be made and stored.

The Headteacher may accept the payment in instalments.

If the payment has not been made after six weeks, the fee will increase by five percent and continues for a maximum of six months – at which point formal disciplinary procedures will begin.

The member of staff will not be permitted to access school-owned electronic devices until the payment has been made.

In cases where a member of staff repeatedly damages school-owned electronic devices, the Headteacher may decide to permanently exclude the member of staff from accessing devices.

If a school-owned device is lost or stolen, or is suspected of having been lost or stolen, the DPO will be informed as soon as possible to ensure the appropriate steps are taken to delete data from the device that relates to the school, its staff and its students, and that the loss is reported to the relevant agencies.

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

15.External IT supplier contact details:

Eitex 01977 804 928 or support@eitex.co.uk

16.Implementation

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

Regular monitoring and recording of email messages may be carried out on a random basis. Hard copies of email messages can be used as evidence in disciplinary proceedings.

Use of the telephone system may be logged and monitored.

Use of the school internet connection may be recorded and monitored.

The Operations Director will conduct random checks of asset registered and security marked items.

The external IT supplier can check computer logs on the school network.

Unsuccessful and successful log-ons will be logged on every computer connected to the school's network.

Unsuccessful and successful software installations, security changes and items sent to the printer may also be logged.

The external IT supplier 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 with a centralised administration package; any virus found will be logged to this package.

The school's database systems are computerised. Attempting to access the database 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 Operations Director and the external IT supplier.

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 Operations Director and the Headteacher.

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

The scheduled review date for this policy will be June 2027