THE SOCIETAS TRUST

Staff ICT and Electronic Devices Policy

Date of Policy	2025
Reviewed and Agreed by	The Directors' Board
Review Date	October 2025
Next Review Date	Autumn 2026

Contents:

Statement of intent

The Societas Trust 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 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 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.
- A process is in place for claiming financial payments when electronic devices are lost or damaged by members of staff.

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
- Data Retention Policy
- Freedom of Information Policy
- Complaints Policy
- Disciplinary Policy and Procedure
- Online Safety Policy
- Photography and Images Policy
- Cyber Crime Response Plan 2023

2. Roles and responsibilities

The Governing Board 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 ICT technician and Compliance and Training Manager, 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. This duty is carried out by the ABM.
- Handling complaints regarding this policy as outlined in the school's Complaints Policy.
- Informing staff that the school reserves the right to access personal devices for the purpose of ensuring the effectiveness of this policy.

The ICT technician is responsible for:

- Carrying out regular checks on internet activity of all user accounts and to report any inappropriate use to the headteacher.
- Monitoring the computer logs on the school's network and to report any logged inappropriate use to 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 and personal devices that have been approved for work purposes (ie. with monitoring software installed) 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.
- Disciplinary measures may be taken with staff who do not follow this policy.
- 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.

The Headteacher is responsible for:

- Ensuring that all school-owned and approved personal electronic 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 or are password protected.
- Ensuring all staff are aware of, and comply with, the data protection principles outlined in the school's Data Protection Policy.

Staff members are responsible for:

- Requesting permission from the headteacher or ICT technician, 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 ABM.
- Ensuring any personal devices that are connected to the school network are encrypted or are password protected.
- Reporting misuse of ICT facilities or devices, by staff or pupils, to the headteacher.
- Reading and signing a Device and Technology Acceptable Use Agreement for staff to confirm they understand their responsibilities and what is expected of them when they use school-owned and personal devices.

The ABM is responsible for the maintenance and day-to-day management of the equipment, as well as the device loans process.

The ABM is responsible for:

- 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.

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
- 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
- Pagers
- Fax equipment
- 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 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 ICT and related equipment.

Since ICT facilities are also used by pupils, the school has a Device and Technology Acceptable Use Agreement for Pupils – staff will ensure that pupils comply with these.

Pupils 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:

- 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 ICT technician.
- 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.

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 are 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 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. Staff will be made aware that network and internet activity is logged and monitored and can be made available, on request, to the Headteacher in the event of allegations of misconduct.

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 lasting less than 10 minutes. A charge may be requested as a result of calls exceeding this time.

Should staff need to use the telephones for longer than this, authorisation will be sought from the headteacher. This authorisation will be requested on each occasion. The exception to authorisation is the use of the telephone system to make personal emergency calls; however, staff will notify the headteacher after the call.

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.

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 Device and Technology Acceptable Use Agreement for Staff.

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 proof read 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 two years dependent on the information contained. 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 school hours and only if they have built-in anti-virus protection approved by the ICT technician. Staff will ensure that access to personal emails never interferes with work duties.

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

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

6. Portable Equipment

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

Portable school-owned electronic devices will not be left unattended, and instead will be kept out of sight and securely locked in location 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, laptops and personal digital assistants, for off-site visits and trips, staff and authorised pupils will only use these devices.

7. Personal devices

Staff members will use personal devices in line with the school's Data and Cyber-security Breach Prevention and Management Plan.

Staff approved to use their own devices will be aware that monitoring software is installed and the possibility of their personal information being seen by the ICT technician.

Staff accessing personal emails on school devices will be aware that monitoring software is installed and the possibility of their personal email information being seen by the ICT technician.

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

Members of staff will not contact pupils or parents using their personal devices.

Personal devices will only be used for off-site educational purposes when mutually agreed with the headteacher.

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.

During lesson times, personal devices will be kept securely in location.

Removable media

Removable Media storing Data must only be used as a last resort, when all other options have been considered, including the need to store or process the data or the secure network service is not available.

Only Removable Media provided by the Academy or Trust that has been encrypted should be used for the storing of Data.

Removable Media should not be used for the storing of Personal Data, Special Category or Sensitive Data unless the device is capable of and has been encrypted.

Removable Media must be stored securely.

If Removable Media used for, or in connection with Academy business is lost or stolen, the loss/theft should be reported to Data Protection Officer and IT Support Team immediately. Where possible the Personal Device should be remotely accessed and the information erased.

8. 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. Further information can be found in the Trust Information Security Policy.

9. 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 two years.

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 ICT technician.

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.

10. 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 ICT technician or headteacher. Certain items are asset registered and security marked; their location is recorded by the ABM for accountability. Once items are moved after authorisation, staff will be responsible for notifying the ABM of the new

location. The exception to this point is when items are moved to the designated secure room for insurance purposes over holiday periods.

- 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. It is recommended that the password are changed at least every three months. 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 hardware or software without the consent of the ICT technician or the headteacher.
- 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 ICT technician 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 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. 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.
- 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.
- Use the ICT 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.

11. Loaning electronic devices

School equipment, including electronic devices, will be loaned to staff members in line with the school's Loaning School Equipment Policy.

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 will be five working days; however, where required, this can be extended following discussion with the ABM or headteacher.

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

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

12. Purchasing

The ABM 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 ABM, including any accessories which were originally included with the device. Any old devices will then be disposed of or wiped clear by the ICT technician.

13. Safety and security

The school's network will be secured in line with the Information Security Policy and Cyber Response Plan.

Filtering of websites, as detailed in the Information Security Policy and Cyber Response Plan, will ensure that access to websites with known malware are reported to the ICT technician and blocked immediately.

Malware detection is included in antivirus software and is updated automatically.

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 termly basis.

Approved personal devices will also be submitted on a termly basis, to the ICT technician, so that appropriate security and software updates can be installed to prevent any loss of data. Consent for such access will be obtained before the approval of a device – if consent if refused, the school reserves the right to decline a request to use a personal device.

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

Members of staff who install or remove software from a school-owned electronic device without seeking authorisation from the ICT technician, 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. This will be no more than 10 minutes for mobile or other portable devices and 15 minutes for desktop computers or laptops.

All devices must be encrypted using a method approved by the IT Technician/Headteacher.

Further security arrangements are outlined in the Information Security Policy and Cyber Response Plan.

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 ICT technician
- 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 ICT technician and headteacher will decide whether a device has been damaged due to the actions described above.

The ICT technician 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 ABM via the **main office**, and a receipt is given to the member of staff.

The school will accept payments made via credit and debit cards, cheques and cash.

A record of the payment will be made and stored in the **main office** for future reference.

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 headteacher 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 pupils, 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. Implementation

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

Regular monitoring and recording of email messages will 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 will be logged and monitored.

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

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

The ICT technician will check computer logs on the school network on a termly basis.

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 will also be logged.

The school's network has anti-virus software installed with a centralised administration package; any virus found will be logged to this package.

User accounts will be accessible by the headteacher and the ICT technician.

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.

A. Device and Technology Acceptable Use Agreement for Staff

This agreement outlines staff members' responsibilities when using technology and devices, both school-owned and personal, and applies to all staff, volunteers, contractors and visitors.

The setting will ensure that any monitoring activities undertaken are lawful and fair to workers, as well as meet data protection requirements.

If any monitoring activities are undertaken, then the setting will ensure that employees are made aware of the nature, reasons, and extent of the monitoring, that the monitoring has a clearly defined purpose, and that it is as un-intrusive as possible to the employees. The setting will also ensure that all suitable safety checks are carried out prior to monitoring activities.

Please read this agreement carefully, and sign at the bottom to show you agree to the terms outlined.

Data protection and cyber-security

I will:

- Use technology and devices, including the use and storage of personal data, in line with data protection legislation, including the Data Protection Act 2018 and UK GDPR.
- Follow the **Data Protection Policy** and any other relevant setting policies and procedures.

I will not:

- Attempt to bypass any filtering, monitoring and security systems.
- Share setting-related passwords with pupils, staff, parents or others unless permission has been given for me to do so.

Using technology

I will:

- Follow the **Staff ICT and Electronic Devices Policy**.
- Only use ICT systems which I have been permitted to use.
- Ensure I obtain permission prior to accessing materials from unapproved sources.
- Only use the internet for personal use during out-of-setting hours, including break and lunch time.
- Only use encrypted Removable Media to store Data as a last resort, when all other options have been considered.

I will not:

- Install any software onto setting ICT systems unless instructed to do so by the headteacher or ICT technician.
- Search for, view, download, upload or transmit any inappropriate material when using the internet.

Emails

I will:

- Only use the approved email accounts that have been provided to me when sending communications regarding setting business.
- Ensure any personal information that is being sent via email is only sent to the relevant people and is appropriately protected.

I will not:

- Use personal emails to send and/or receive setting-related personal data or information, including sensitive information.
- Use personal email accounts to contact pupils or parents.

School-owned devices

I will:

- Only use school-owned devices for the purpose of carrying out my school responsibilities.
- Only access websites and apps that have been approved by the **headteacher**.
- Understand that the usage of my school-owned devices will be monitored.
- Provide suitable care for my school-owned devices at all times.
- Only communicate with pupils and parents on school-owned devices using appropriate channels.
- Ensure I install and update security software on setting-owned devices as directed by the **ICT technician**.
- Only take photos and videos of pupils using the school's digital cameras; however, I may use other school-owned devices, such as mobile phones and tablets, where the ABM has been consulted and consent has been given by the headteacher prior to the activity.
- Immediately report any damage or loss of my school-owned devices to the ABM or ICT Technician.
- Immediately report any security issues, such as downloading a virus, to the ABM or ICT technician.
- Understand that 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.
- Understand that I will use school-owned electronic devices within the parameters of the school's insurance cover.
- Make arrangements to return setting-owned devices to the ABM upon the end of my employment at the setting.

I will not:

- Permit any other individual to use my school-owned devices without my supervision, unless otherwise agreed by the **headteacher**.
- Install any software onto setting-owned devices unless instructed to do so by the **headteacher** or **ICT technician**.
- Use school-owned devices to send inappropriate messages, images, videos or other content.
- Use school-owned devices to view, store, download or share any inappropriate, harmful or illegal content.
- Use school-owned devices to access personal social media accounts.

Personal devices

I will:

- Only use personal devices during out-of-setting hours, including break and lunch times.
- Ensure personal devices are either switched off or set to silent mode during setting hours.
- Only make or receive calls in specific areas, e.g. the staff room.
- Store personal devices appropriately during setting hours, e.g. a lockable cupboard in the classroom.
- Understand that I am liable for any loss, theft or damage to my personal devices.

I will not:

- Use personal devices to communicate with pupils or parents.
- Use personal devices to take photographs or videos of pupils or staff.
- Store any setting-related information on personal devices unless permission to do so has been given by the **headteacher**.

Social media and online professionalism

I will:

- Follow the setting's **Social Media Policy**.
- Understand that I am representing the setting and behave appropriately when posting on setting social media accounts.
- Ensure I apply necessary privacy settings to social media accounts.
- Understand that I am strongly advised to not 'friend' or 'follow' parents on their personal accounts.

I will not:

- Communicate with pupils or parents over personal social media accounts.
- Post any comments or posts about the setting on any social media platforms or other online platforms which may affect the setting's reputability.
- Post any defamatory, objectionable, copyright-infringing or private material, including images and videos of pupils, staff or parents, on any online website.

- Post or upload any images and videos of pupils, staff or parents on any online website without consent from the individuals in the images or videos.
- Give my home address, phone number, mobile number, social networking details or email addresses to pupils or parents – any contact with parents will be done through authorised setting contact channels.

Working from home

I will:

- Ensure I use a portable school-owned device.

Training

I will:

- Participate in any relevant training, including cyber-security and online safety.
- Employ methods of good practice and act as a role model for pupils when using the internet and other digital devices.

Reporting misuse

I will:

- Report any misuse by pupils or staff members breaching the procedures outlined in this agreement to the **headteacher**.
- Understand that my use of the internet will be monitored by the **ICT technician** and recognise the consequences if I breach the terms of this agreement.
- Understand that the **headteacher** may decide to take disciplinary action against me, in accordance with the **Disciplinary Policy and Procedure**, if I breach this agreement.

Agreement

I certify that I have read and understood this agreement, and ensure that I will abide by each principle.

Name	
Signature	
Date	

B. Loan Request Form

Loan Request Form

This form should be completed by staff members when requesting to loan school-owned equipment.

Staff members must detail the specific equipment or device which is requested, as well as provide a reason, and where necessary, evidence, as to why the equipment or device is required.

The completed form should be returned to the ABM for authorisation.

Name		**Department**	
Equipment required			
Reason			
First date of loan		**Return date**	
Authorised (if rejected, detail why)			
Signed (DEL)			
Job role		**Date**	