

Policy Author	Mr K Hopkins	Date of Approval	29.09.25
Policy Approval	Full Governing Board	Next Review Date	September 2026

## Statement of Intent

Oldbrook First School and Nursery 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 Online Safety Policy.

## 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
- Complaints Procedures Policy
- Disciplinary Policy and Procedure
- Online Safety Policy
- Photography and Images Policy
- Finance Policy

## 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 DPO, 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 Headteacher.
- 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 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 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.
- 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 DPO.

The DPO is responsible for:

- 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.
- Requesting permission from the headteacher, subject to their approval, before using personal devices during school hours.
- Ensuring any personal devices that are connected to the school network are encrypted in a manner approved by the DPO.
- Reporting misuse of ICT 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.

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

The SBM 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.

## 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
- Visualisers
- Internet (email, web access and video conferencing)
- Telephones (fixed and mobile)
- Tablets and other portable devices
- Photocopying and printing
- Recording and playback equipment

## 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 will have acceptable use agreements in place 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:

- Open email attachments from unknown sources.
- Use programmes or software that may allow them to bypass the filtering or security systems.
- 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.

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 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 will be taken home for work purposes only, once approval has been sought from the headteacher. 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.

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.

## **Emails**

The school email system is 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. 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.

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

All emails that are sent or received will be retained within the school for a period of six months dependent on the information contained.

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 Headteacher 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.

Contracts sent via email or the internet are as legally binding. 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.

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 the Financial Management Policy.

### **Portable Equipment**

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

Portable school-owned electronic devices will not be left unattended, and instead will be kept out of sight and securely locked when they are not in use. Portable equipment will be transported in its protective case, if supplied.

### **Personal devices**

All personal devices that are used to access the school's systems or email accounts, e.g. laptops or mobile phones, will be declared and approved by the headteacher before use.

Staff using their own devices will sign an agreement stating that they understand the requirement to keep information safe and the appropriate security measures for this. 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. Members of staff bringing personal devices into school will ensure that there is not any inappropriate or illegal content on their device.

Personal devices must not be used within the main teaching areas or around children and should be kept locked away in staff lockers when not in use.

### **Removable media**

Only recommended removable media will be used including, but not limited to, portable drives and USB drives. All removable media will be securely stored when not in use and must be encrypted. Personal and confidential information will not be stored on any removable media. Removable media will be disposed of securely by the Headteacher.

### **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.

### **Messages**

Emails and messages stored on school-owned devices will be stored digitally. 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 Headteacher.

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.

### 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 SBM for accountability.
- 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. The password will be changed every six 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, including online chat or adult sites.
- 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 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.
- 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 otherwise known as "upskirting".

Staff must report any concerns to the Headteacher immediately. Any unauthorised use of email or the internet will likely result in disciplinary action, in line with the Disciplinary Policy and Procedure.

### Loaning Electronic Devices

School equipment, including electronic devices, will be loaned to staff members in line with the school's Loan Agreement. 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 agreement. By loaning school equipment and electronic devices, staff members will be agreeing to act in accordance with the terms of acceptable use. Training will be provided where necessary for equipment, including how to store, handle and undertake any maintenance.

If the equipment or device is no longer required, staff members will return the equipment to the Headteacher 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.

### Safety and Security

The school's network will be secured using firewalls in line with data and cyber-security requirements. Filtering of websites, will ensure that access to websites with known malware are blocked immediately and reported to the ICT technician. Approved anti-virus software and malware protection will be used on all approved devices and will be updated on a termly basis. The school e-mail has spam and malware protection.

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.

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

### 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 Headteacher
- 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. 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 towards the costs. 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.

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 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.

## Implementation

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

Regular monitoring of email messages will be carried out. Hard copies of email messages can be used as evidence in disciplinary proceedings.

Use of the telephone system will be monitored.

The SBM will conduct checks of asset registered and security marked items annually.

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

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

The ICT technician 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.

All users of the school's MIS will be issued with a unique individual login and password, which will be changed regularly. Staff will not, under any circumstances, disclose this password to any other person. Attempting to access the MIS 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 ICT technician inline with this policy and when permission has been granted by the Headteacher for any matter where a breach of policy is thought to have taken place.

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 misuse or breach of the rules in this policy may result in disciplinary action and could also result in criminal or civil actions being brought against the persons involved or the school.

## Staff Declaration Form

All members of staff are required to sign this form before they are permitted to use electronic devices that are owned by the school.

By signing this form, you are declaring that you have read, understood and agree to the terms of the Internet and Acceptable Use Policy. You should read and sign the declaration below before returning it to the school office.

Members of staff are required to re-sign this declaration form if changes are made to the policy.

---

I have read the policy and understand that:

- School equipment must not be used for the fulfilment of another job or for personal use, unless specifically authorised by the headteacher.
- Illegal, inappropriate or unacceptable use of school or personal equipment will result in disciplinary action.
- The school reserves the right to monitor my work emails, internet activity and document production.
- Passwords must not be shared and access to the school's computer systems must be kept confidential.
- I must act in accordance with this policy at all times.

<b>Name of staff</b>	
<b>Job title</b>	
<b>Department</b>	
<b>Signed</b>	
<b>Headteacher signed</b>	
<b>Date signed</b>	

## Device and technology acceptable use agreement for staff

Whilst our school promotes the use of technology or devices, and understands the positive effects they can have on enhancing pupils' learning and community engagement, we must also ensure that staff use technology and devices appropriately. Any misuse of technology and devices will not be taken lightly and will be reported to the headteacher in order for any necessary further action to be taken.

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 school will ensure that any monitoring activities undertaken are lawful and fair to workers, notifying staff of the nature or reason as well as meet data protection requirements.

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 school's Data Protection Policy and any other relevant school policies and procedures.

I will not:

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

### Using technology in school

I will:

- Follow the Internet and Acceptable Use Policy and Online Safety 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 professional use
- Only use recommended removable media and keep this securely stored following the permission of the headteacher.

I will not:

- Install any software onto school 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 school 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 school-related personal data or information, including sensitive information.
- Use personal email accounts to contact pupils or parents.

Together we make the difference

## School-owned devices

I will:

- Only use school-owned devices for the purpose of carrying out my school responsibilities.
- Only access apps that have been approved by the headteacher.
- Understand that the usage of my school-owned devices will be monitored.
- Keep my school-owned devices with me or store them securely when not in use.
- Transport school-owned devices safely and 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 school-owned devices as directed by the ICT technician.
- Only use school-owned devices to take and store photographs or videos of pupils, parents, staff and visitors for the intended purpose of school related activity.
- Immediately report any damage or loss of my school-owned devices to the Headteacher.
- Immediately report any security issues, such as downloading a virus, to the ICT technician and Headteacher.
- Understand that I am expected to pay an excess for any repair or replacements costs where the device was damaged or lost as a result of my own negligence.
- Make arrangements to return school-owned devices to the Headteacher upon the end of my employment at the school.

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 school-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-school hours, including break and lunch times.
- Ensure personal devices are either switched off or set to silent mode during school hours.
- Only make or receive calls in specific areas, e.g. the staff room.
- Store personal devices appropriately during school hours, e.g. locker
- 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.
- Access the school's Wi-Fi using a personal device unless permission to do so has been granted by the headteacher or ICT technician.
- Use personal devices to take photographs or videos of pupils, parents or staff.
- Store any school-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 school's policies.
- Understand that I am representing the school and behave appropriately when posting on school social media accounts.
- Ensure I apply necessary privacy settings to social media accounts.

I will not:

- Communicate with pupils or parents over personal social media accounts.
- Accept 'friend' or 'follow' requests from any pupils or parents over personal social media accounts.
- Post any comments or posts about the school on any social media platforms or other online platforms which may affect the school'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 school contact channels.

### Working from home

I will:

- Ensure that a school based device is used when working from home.
- Ensure I obtain permission from the headteacher before any personal data is transferred from a school-owned device to a personal device.
- Ensure any data transferred from a school-owned device to a personal device is encrypted or pseudonymised.
- Ensure any sensitive personal data is not transferred to a personal device.
- Ensure no unauthorised persons, such as family members or friends, access any personal devices used for home working.

### Training

I will:

- Participate in any relevant training offered to me, 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 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.

<b>Name</b>	
<b>Signature</b>	
<b>Date</b>	