Internet and Acceptable Use Policy

Policy Author	**Mr K Hopkins**	**Date of Approval**	28.09.26
Policy Approval	**Full Governing Board**	**Next Review Date**	September 2027

DSL	**Mr K Hopkins**	**Responsible Governor**	Mrs Val Powell
Deputy DSL	**Mrs Rachael Dunkley**	**ICT Technician**	Mr Robet De Atouguia

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 fair process is in place for reporting loss or damage and considering any lawful recovery of costs under the loan agreement.

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)
- Keeping children safe in education 2026 (KCSIE);
- Working together to safeguard children 2026;
- the September 2026 EYFS framework for group and school-based providers;
- Mobile phones in schools statutory guidance [1, 2, 6, 7]

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
- Child Protection and Safeguarding Policy
- Staff Code of Conduct
- Low Level Concerns Policy
- Whistleblowing
- Behaviour Policy
- Medical Needs Policy

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 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.
- Allocating sufficient resources for secure technology, staff training and timely safeguarding responses.
- 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:

- Maintaining the technical filtering and monitoring arrangements, providing reports to the DSL and promptly escalating safeguarding alerts. Technical staff must not decide safeguarding outcomes alone.
- Reviewing security logs at a risk-based frequency and acting promptly on alerts. Safeguarding alerts must reach the DSL or deputy without waiting for a periodic technical review.
- Providing authorised remote support or investigation through access-controlled, logged tools. Tell the user before a support session where practicable; use only the access necessary for the task. Any exceptional covert investigation requires specific legal and data-protection assessment and senior authorisation.
- Maintaining security on managed devices, and checking approved personal-device work access against the agreed security requirements without unnecessary access to personal information.
- Explaining the scope of approved checks and monitoring before work access is enabled, and protecting any private information incidentally encountered.
- 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 suspected personal-data breaches to the DPO and Headteacher, and any associated child-safety risk to the DSL.

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.

Designated safeguarding lead and governance are responsible for:

The DSL leads online safeguarding, with deputy cover, and assesses alerts and incidents, makes referrals and ensures children receive support. The Headteacher, DSL and ICT technician must agree who checks alerts, response times, absence cover and arrangements outside school hours.

The Governing Board must receive assurance on online safety and have identified a responsible governor and senior leader for filtering and monitoring.

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.
- Using personal devices for work only where a written, risk-assessed exception has been approved under this policy, including encryption, supported software and separation of school data.
- Reporting safeguarding concerns immediately to the DSL or deputy, technical incidents to the ICT technician and Headteacher, and personal-data breaches to the DPO. Adult-conduct concerns follow the routes below.
- 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

ntable use

This policy applies to employees, governors, volunteers, contractors and visitors using school systems, accounts, networks or devices, on or off site. It also covers approved personal-device work access and online conduct affecting pupils, professional duties or school information. Pupil use is supported through age-appropriate rules and supervision.

School systems and work activity may be monitored in accordance with the safeguards below. Approved use includes the following work and educational purposes; any personal use remains subject to the limited permissions in this policy:

- 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.

Suspected misuse will be assessed fairly under the relevant safeguarding, data-protection and disciplinary procedures. A breach may lead to proportionate disciplinary action; outcomes are not automatic and do not replace safeguarding referrals.

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.

Staff will teach and revisit age-appropriate pupil acceptable-use rules, supervise activity and make suitable adjustments for SEND. Report concerns to the DSL as well as the Headteacher where safeguarding may be involved. A child reporting harmful content must be supported, not blamed for seeking help.

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

Immediately report illegal, inappropriate or harmful activity through the incident-response routes below. Do not investigate suspected child abuse by opening or circulating images.

Members of staff will not:

- Open suspicious links, attachments or QR codes, enable macros, or enter credentials in response to an unexpected request without checking through a trusted route. A familiar sender name does not establish authenticity.
- 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 confidential information or posting abusive, discriminatory, harassing or defamatory material. These rules do not prevent protected disclosures, lawful whistleblowing, reporting safeguarding concerns, seeking professional advice or lawful trade union activity.
- Apply appropriate privacy settings, while recognising that private posts and messages may be copied or shared.

Publish images only through approved school channels for a documented purpose and lawful basis, following the Photography and Images Policy and recorded permissions or restrictions. Obtain consent where required; consider the child's wishes, safeguarding risk and the possibility of AI misuse. Do not pair identifiable images with unnecessary location, timetable or other personal details.

Copyrighted material may be used only with an appropriate licence, permission or applicable legal exception. Check restrictions before copying, downloading, publishing or uploading it to an AI service.

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.

The staff declaration and acceptable-use agreement at the end of this policy form part of these requirements and must be read consistently with the policy.

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.

Retain email and messages according to their content, purpose and the approved retention schedule, not a blanket six-month rule. Save safeguarding, employment and other records in the appropriate secure system. Suspend routine deletion where required for an investigation, complaint, legal hold or information request, then dispose of records securely when no longer needed.

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.

Work email on a personal device is permitted only under the written exception and security controls in the Personal devices section. Approval is not permission to use personal email accounts for school business or to store uncontrolled local copies.

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.

Report suspicious emails promptly to the ICT technician and Headteacher using the approved reporting route, and to the DSL or DPO where relevant. Do not forward suspected abusive images or open attachments to investigate.

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

Store school information only on approved managed storage, with backups, restricted access and tested recovery arrangements. The ICT technician will maintain protected backups, including a copy isolated from ordinary accounts and ransomware, and record restoration tests.

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

School-managed devices are the default for school work and home working. Any personal-device work access requires prior written Headteacher approval, DPO advice and ICT checks, defining the permitted purpose, data, access method, security controls and end date. Personal email, personal cloud storage and unapproved local downloads remain prohibited.

Approved personal-device access must use supported and updated software, encryption, screen lock, appropriate malware protection and approved authentication. Keep work information in a managed account or container; prevent family or other third-party access. Explain any remote removal of school data in advance and limit it to that data wherever possible. The school has no general entitlement to private passwords, messages, photographs or unrestricted device searches. Use only school-owned devices and approved channels to contact pupils or parents.

Personal phones, cameras, smartwatches and other devices with recording, imaging or sharing capabilities must not be used in teaching or childcare areas or around children, and must be securely stored when not in use in lockers. Personal use is confined to breaks or non-working time in designated staff room. Any necessary medical, accessibility or work-authentication exception must be agreed, risk assessed and must not compromise supervision or image safeguards. Visitors are told these rules.

Pupils mobile devices and early years

Pupils must not use personal mobile phones or similar connected devices during the school day, including breaks. If a device must be brought to school, it is switched off and handed to the school office for secure storage and return at collection. Agree necessary disability, medical or other exceptional access individually; never remove an essential medical aid. Parents contact children through the office. Apply the Behaviour Policy and lawful searching and confiscation guidance; this policy does not grant unlimited powers to search devices. [7]

In nursery and Reception, we apply the current EYFS rules on phones, cameras and devices with imaging or sharing functions. We take and store children's images only on approved school equipment for an authorised purpose; personal devices and personal accounts must not be used. We brief visitors and contractors and challenge unauthorised recording. [6]

From September 2026, EYFS paragraph 3.94 requires providers to have regard to DfE's early-years screen-use guidance. The early-years lead will review screen use against it: use screens purposefully with adult support, choose suitable content and avoid replacing interaction, play, movement and hands-on learning. We will discuss consistent approaches with families. [6]

For nursery children, we will avoid screen time below age two except exceptional use; for ages two to five, we will work with parents towards no more than one hour daily across home and the setting, preferably less. Essential SEND assistive technology is excluded from these limits. We will ensure we preview content, choose advert-free material without scrolling or autoplay, co-engage throughout, and avoid background screens or use for behaviour management.

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.

Storing 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 account or share their own password, MFA code or recovery code. Use unique, strong credentials or approved passkeys. Change credentials immediately if compromised or suspected of compromise; routine six-month changes are not the default. Use approved password-management and account-recovery arrangements.
- 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 constitutes bullying, harassment, unlawful discrimination, a threat or other abuse, including online sexual harassment.
  - 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.
  - Defamatory, threatening, abusive or unlawfully discriminatory material.
- Generate messages or documents that appear to originate from someone else, or otherwise impersonate someone else.
- Post comments or material that may contain misinformation, disinformation or conspiracy theories.

- Use Generative AI for any other purposes that are not related to teaching and their role.
- 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 introduce or distribute malicious code or compromise school systems. Report accidental exposure immediately; disciplinary decisions will follow a fair process.
- 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".

Report concerns immediately using the appropriate safeguarding, technical, data-protection or adult-conduct route below. Misuse may result in action under the relevant procedure after fair assessment.

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, maleware protection and secure configuration 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. Staff will use individual accounts with only the access needed for the role, lock screens when unattended and keep privileged administration separate from everyday work.

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 must follow the loan agreement and take reasonable care of school equipment, including when travelling or working at home.

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.

Any proposed recovery of loss or damage costs must be considered fairly under the loan agreement and applicable employment law.

Report loss or theft, including suspected loss, immediately to the Headteacher and ICT technician and to the DPO where personal data may be involved. Authorised staff will assess containment, access revocation, remote lock or erasure and preservation of evidence, coordinating with police where needed. Do not delay the report while trying to recover the device.

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.

Filtering monitoring and online safety

Leaders and staff will assess content, contact, conduct and commercial risks, including scams, grooming, bullying, exploitation, harmful challenges, extremism and AI-generated abuse. Staff will adapt teaching and support to pupils' age, SEND and vulnerabilities. Staff supervision and a trusted reporting culture remain essential; no filter can guarantee safety. [1]

The annual review must cover devices used at home, guest access, user groups and dynamic or AI-generated content. Leaders will record risk-based checks and actions, recheck after changes, and document authorised filtering exceptions with an expiry date. We will avoid unnecessary blocking of learning; users must not bypass controls using VPNs, proxies, hotspots or unauthorised accounts. Any approved security testing must be explicitly authorised. [3]

The school will explain to parents how school devices and remote learning are protected, the limits of school coverage and how to report concerns. The computing curriculum provides age-appropriate teaching about privacy, respectful behaviour, misinformation and getting help. Staff receive online safety, filtering and monitoring training at induction and updates. All staff must read KCSIE 2026 Part one in full. [1]

Artificial intelligence and new digital services

Only use approved AI tools for an approved school purpose. Before adoption, the Headteacher, DSL, ICT technician and DPO must assess suitability, age restrictions, accessibility, security, data use, retention and safeguarding, including embedded AI features. Staff will use the DfE product safety standards when evaluating products; approval of a website does not automatically approve every new AI feature. [5]

Do not enter identifiable pupil, family or staff information, safeguarding records, images, confidential material or pupil work into an unapproved AI tool. Any strictly necessary personal-data use requires a documented lawful basis, appropriate contractual controls, privacy information and a DPIA where required. Prevent provider training on school data unless separately lawfully authorised. [5]

Staff remain responsible for checking accuracy, bias, suitability and copyright before using AI output. AI must not make safeguarding, disciplinary or other significant decisions about individuals without meaningful authorised human assessment. Record material AI assistance where needed for transparency and accountability. Do not use AI to impersonate people, fabricate evidence or create sexualised images. [5]

Early-years children must not use AI tools or AI-enabled toys, in line with the screen-use guidance. Older pupils may use AI only in a specifically approved, age-appropriate activity under close supervision, with effective safeguards. Do not allow pupils to open under-age accounts. General-purpose unsupervised chatbot use is not permitted by this policy. [5]

Responding to incidents and concerns

Reassure and protect the child; stop the activity if needed. Report immediately to the DSL or deputy and record facts, time, account or web address and action taken to safeguard. Do not promise secrecy or investigate a disclosure yourself. If a child is in immediate danger call 999; make a prompt social-care or police referral where required. [1, 2]

For suspected nude, semi-nude or sexual abuse imagery involving a child, including AI-generated or altered images, do not intentionally view, copy, print, screenshot, save, forward or ask anyone to send it. Do not ask a child to show it or instruct deletion before the DSL has considered evidence and police advice. Secure the device or account as directed without exploring the content. The DSL will follow UKCIS guidance, including the exceptional viewing criteria, recording decisions and referral thresholds. [8]

Concerns about an adult's conduct must be reported to the Headteacher, or Chair of Governors for the Headteacher, under KCSIE Part four and the school's allegations/low-level-concerns procedures. The Headteacher will seek LADO advice where the harm threshold may be met or classification is uncertain.[1]

For suspected malware, account takeover or data loss, stop using the affected service immediately and inform the DSL who will contact IT immediately through a trusted route. Follow the incident plan on safe isolation; do not wipe devices, delete logs or attempt an improvised recovery. IT and leaders will coordinate containment, recovery, notifications and continuity of safeguarding and school operations.

The DPO advises the school on personal-data breaches. Record every breach and assessment. The Headteacher will notify the ICO without undue delay and, where feasible, within 72 hours of awareness unless the breach is unlikely to risk individuals' rights and freedoms. The Headteacher will inform affected people without undue delay where high risk requires it. An incomplete investigation must not delay an initial required report. [10]

The DSL will share necessary safeguarding information lawfully and securely; uncertainty over consent must not delay protection. [2, 11]

Implementation and review

The Headteacher will provide an accessible route to the DPO for concerns about personal-data use, monitoring or AI. Complaints will be handled promptly under the school's data-protection complaints process and escalation rights will be explained.

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 schoo l.

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 may result in proportionate action under the relevant safeguarding or disciplinary procedure following fair assessment.
- Work activity may be monitored only for the lawful, necessary and proportionate purposes and safeguards explained in this policy and the staff privacy notice.
- 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.

Name of staff	
Job title	
Department	
Signed	
Headteacher signed	
Date signed	

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.

Monitoring is subject to the lawful, fair and proportionate arrangements in this policy and the staff privacy notice. My signature confirms that I understand these arrangements.

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 passwords, MFA codes or recovery codes, or allow another person to use my account. Authorised delegation and account recovery must use the approved technical process.

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.

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 the scope and limits of lawful monitoring explained in this policy and the privacy notice.
- 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 damage, loss or theft to the Headteacher and IT technician, and to the DPO if personal data may be involved.
- Immediately report cyber incidents to the IT technician and Headteacher, safeguarding concerns to the DSL or deputy, and personal-data breaches to the DPO.
- Understand that any proposed recovery of costs must follow a fair process, the loan agreement and employment law.
- Make arrangements to return school-owned devices to the Headteacher upon the end of my employment at the school.

I will not:

- Allow unauthorised people, including family members, to use school devices or accounts. Any shared educational use must be specifically approved and use appropriate access controls.
- 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:

- Use personal devices only during breaks or non-working time in the designated staff room, unless subject to an agreed medical, accessibility or essential work-authentication exception.
- Keep personal devices silent or switched off and securely stored in allocated lockers while working with children, subject to an agreed exception.
- Only make or receive calls in specific areas, e.g. the staff room.
- Store personal devices appropriately during school hours in a school 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 school information on a personal device or personal cloud service. Any exceptional work access must follow the written approval, managed storage and security controls in this policy; Headteacher permission alone is not enough.

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 abusive, discriminatory, defamatory or confidential material. This does not restrict lawful whistleblowing, safeguarding reports, professional advice or protected disclosures.
- 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.
- Use only approved managed storage and remote access. Any personal-device exception must be documented and meet all the policy's security and data-protection conditions.
- Keep authorised work access protected by encryption, access controls and approved authentication.
- Ensure any sensitive personal data is not transferred to a personal device.
- Prevent family members, friends or other unauthorised people from accessing work devices, accounts or information.
- I will use only approved AI tools, protect school data, check outputs and comply with the AI safeguards in this policy.
- I will follow filtering and monitoring controls and report weaknesses promptly rather than attempting to bypass them.
- I will not intentionally view, copy or circulate suspected child sexual abuse imagery, including AI-generated images, and will refer immediately to the DSL.

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 the lawful monitoring arrangements and report accidental exposure or mistakes promptly so the school can protect people and systems.
- 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	