Whitecross Nursery School

Staff ICT & Electronic Devices Policy

Reviewed by	Claire FitzPatrick & LeadIT
Date of last review	March 2024
Date of next review	March 2025
Ratified by the Governing Body	Tuesday 26th March 2024

This policy will be reviewed sooner if there is a change to legislation or guidance which may affect it. Any changes will be communicated to all stakeholders.

Statement of intent

Whitecross Nursery School 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 children 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 are not permitted at Whitecross Nursery School.

1. Legal framework

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

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

This policy operates in conjunction with the following school policies:

- Data Protection Policy
- Freedom of Information Policy
- Complaints Procedures Policy
- Disciplinary Policy and Procedure
- Online Safety Policy
- Loaning School Equipment Policy
- Photography and Images Policy
- Data and Cyber-security Breach Prevention and Management Plan
- Finance Policy
- Records Management Policy

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 SBM and LeadIT, taking into account new legislation, government guidance and previously reported incidents, to improve procedures.
- The day-to-day implementation and management of the policy.
- Handling complaints regarding this policy as outlined in the school's Complaints Procedures Policy.

LeadIT 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 devices 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.
- Ensuring that all school-owned and 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.
- Ensuring all staff are aware of, and comply with, the data protection principles outlined in the school’s Data Protection Policy.
- The maintenance and day-to-day management of the equipment.

Staff members are responsible for:

- Reporting misuse of ICT facilities or devices, by staff or children, 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 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.

3. Classifications

School-owned devices or include, but are not limited to, the following:

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

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 children, serving as a positive role model in the use of ICT and related equipment.

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

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

Members of staff will not:

- Open email attachments from unknown sources.
- Use programmes or software that may allow them to bypass the filtering or security systems.
- Upload or download large capacity files (over 500MB) without permission from
- LeadIT.
- Give their home address, phone number, social networking details or email addresses to children 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 any personal social media accounts.

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

Staff will ensure that 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 children, 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.

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.

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 office 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.

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 **six months** 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. That notice will normally be configured as a signature by LeadIT and will not be removed.

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 the office filling cabinet when they are not in use.

Portable equipment will be transported in its protective case.

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

7. Personal devices

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

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.

During lesson times, unless required for the teaching activity being undertaken, personal devices will be kept in staff lockers.

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; therefore, members of staff will ensure that cloud-based data is kept confidential and no data is copied, removed or adapted.

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 six months.

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 LeadIT.

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 Headteacher. Certain items are asset registered and security marked; their location is recorded by the SBM for accountability. Once items are moved after authorisation, staff will be responsible for notifying the SBM 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. 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.
- 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.
- 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.
- 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 children.
- Share any information or data pertaining to other staff or children at the school with unauthorised parties. Data will only be shared for relevant processing purposes.

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 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. Safety and security

The school’s network will be secured using firewalls in line with the Data and Cyber-security Breach Prevention and Management Plan.

Filtering of websites, as detailed in the Data and Cyber-security Breach Prevention and Management Plan, will ensure that access to websites with known malware are blocked immediately and reported to LeadIT.

Approved anti-virus software and malware protection will be used on all approved devices and are updated automatically through L.E.A.D. IT Remote management services.

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

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.

Records will be kept detailing the date allocated, owner of a device and device type, on an audit system – these will be stored in a secure server location and device details are stored on L.E.A.D. IT Remote management systems.

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

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

Members of staff who install or remove software from a school-owned electronic device without seeking authorisation from LeadIT, 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 children, 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 DPO.

Further security arrangements are outlined in the Data and Cyber-security Breach Prevention and Management Plan.

12. 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 LeadIT
- 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.

13. 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 SBM will conduct random checks of asset registered and security marked items.

LeadIT will check computer logs on the school network on a termly basis. Filtering and monitoring services automatically send violation logs to the Headteacher on a weekly 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.

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

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

The school's database systems are computerised. Unless given permission by LeadIT, members of staff will not access the system. Failure to adhere to this requirement may result in disciplinary action.

All users of the database system will be issued with a unique individual password, which will be changed every six months. Staff will not, under any circumstances, disclose this password to any other person.

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

User accounts will be accessible by the Headteacher and LeadIT.

Users will ensure that critical information is not stored solely within the school's computer system. Hard copies will be kept or stored separately on the system. If necessary, documents will be password protected.

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.

14. Monitoring and review

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