ICT Acceptable Use Policy

Policy Approved	**March 2025**
Review Date	**March 2026**
Responsible Staff	**Kara Newton**
Governor	**Andy Avery**

Contents:

Vision Statement

Let your light shine.

Access and ambition for all to enjoy life in all its fullness.

Foundational Scripture

Matthew 5: 16 In the same way, let your light shine before others, that they may see your good deeds and glorify your Father in heaven.

Our school values are rooted in the Sermon on the Mount and are the basis of all relationships, decisions and direction of our school.

School Values

Our school values are at the heart of everything we do. We aim to provide high quality learning opportunities which help foster these values within children. Our values are:

Friendship

Thankfulness

Hope

Unity

Compassion

Forgiveness

Justice

Endurance

Trust

At Hoole Church of England Primary School, we aim to help children become:

- **Enthusiastic, curious, independent thinkers – motivated, reflective and resilient learners** who persevere when faced with challenges and who celebrate their achievements and those of their friends;
- **Respectful, compassionate and kind friends** who are able to work with others, forgive, trust, support and communicate with others;
- **Confident, thankful individuals** who understand their own worth; how to stay safe and healthy and how to manage feelings and relationships;
- **Tolerant and responsible citizens** who show respect for others, and a commitment to appreciate and contribute positively to the world around them.

Statement of intent

Hoole Church of England Primary 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 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.

Staff are provided with electronic devices including laptops and class I-pads.

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 associated policies including the Cybersecurity, Social Media and Online Safety Policies.

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/statements:

- Data Protection Policy
- Freedom of Information Statement
- Complaints Procedures Policy
- Disciplinary Policy and Procedure
- Cybersecurity Policy
- Online Safety Policy
- Data and Cyber-security Breach Prevention and Management Plan
- Device & Technology Acceptable Use Agreement

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 has the overall responsibility for:

- Reviewing and amending this policy with the ICT technician and school business manager, taking into account new legislation, government guidance and previously reported incidents, to improve procedures.
- The day-to-day implementation and management of the policy.
- The overall allocation and provision of resources. This duty is carried out daily by the School Business Manager (SBM).
- 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 School Business Manager, working in collaboration with the school's ICT Technician, is responsible for:

- Carrying out daily 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, working in conjunction with the school's ICT Technician as appropriate. 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 (where appropriate) 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 to the Headteacher and Data Protection Officer (DPO).
- Ensuring that all school-owned 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.

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 additional school equipment and devices from the headteacher or SBM.
- Requesting permission from the headteacher, subject to their approval, before using personal devices during school hours. Please note use of personal devices is restricted to staffroom, staff wellbeing room and office reception area. Personal devices should not be used if pupils are in attendance.
- Ensuring any personal devices that are connected to the school network are encrypted in a manner approved by the SBM.
- Reporting misuse of ICT facilities or devices, by staff or pupils, to the School Business Manager.
- Reading and signing the Device User Agreement to confirm they understand their responsibilities and what is expected of them when they use school-owned devices.

The SBM 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 as per the Manual of Financial Procedures.
- Overseeing purchase requests for electronic devices.

3. Classifications

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

- Computers, laptops and software
- Monitors
- Keyboards
- Mouses
- Scanners
- Cameras
- 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)
- IPads and other portable devices
- Photocopying, printing and reproduction equipment
- Recording and playback equipment
- Documents and publications (any type of format)

4. Acceptable use

This policy applies to any computer or other device connected to the school's network and computers.

All staff are required to sign on an annual basis the Device & Technology Acceptable Use Agreement

The school will monitor the use of all ICT facilities and electronic devices. Members of staff will only use school-owned devices for work duties and educational purposes. The duties for which use is permitted include, but are not limited to, the following:

- Preparing work for lessons, activities, meetings, reviews, etc.
- Researching any school-related task
- Any school encouraged tuition or educational use
- Collating or processing information for school business
- Communicating with other members of staff, such as contacting the school administration team.

Inappropriate use of school-owned devices could result in a breach of the school's Data Protection Policy and/or legislation, including the UK General Data Protection Regulations 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.

Staff will ensure that pupils do not misuse ICT equipment / facilities.

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.
- Upload or download large capacity files (over 500MB) without permission from the ICT technician.
- Give their home address, phone number, social networking details or personal email addresses to pupils or parents – contact with parents will be done through authorised school contact channels.

All data will be stored appropriately in accordance with the school's Data Protection Policy.

Members of staff will only use school-owned electronic devices to take pictures or videos of people who have given their consent.

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

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

Staff will ensure they:

- Express neutral opinions when representing the school online.
- Avoid disclosing any confidential information or comments regarding the school, or any information that may affect its reputability.
- Have the necessary privacy settings are applied to any social networking sites.

Images or videos of pupils, staff or parents will only be published online for the activities which consent has been sought.

Copyrighted material will not be downloaded or distributed.

School-owned allocated devices will be taken home for work purposes only. Remote or cloud based 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. A charge may be made for using equipment if the values are significant.

Where permission has been given to use the school equipment for personal reasons, this use will take place during the employee's own time, e.g. during lunchtime or after school. 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 Device & Technology Acceptable Use Agreement.

Failure to adhere to the rules described in this policy may result in disciplinary action, in line with the Disciplinary Policy and Procedure.

5. Emails and the internet

The school email system and internet connection are available for communication and use on matters directly concerned with school business.

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

Unprofessional messages will not be tolerated. All emails will be written in a professional tone and will be 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. Information classed as sensitive or highly confidential must be transferred using CPOMS (Safeguarding) or Egress (Financial / HR).

The school will be liable for any defamatory information circulated either within the school or to external contacts.

The school email system and accounts will never be registered or subscribed to spam or other non-work-related updates, advertisements or other personal communications. School email addresses will not be shared without confirming that they will not be subjected to spam or sold on to marketing companies.

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

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

Staff linking work email accounts to personal devices is subject to headteacher's approval and may be subject to routine security checks.

The types of information sent through emails to a personal device will be limited to ensure the protection of personal data.

Contracts sent via email or the internet are as legally binding as those sent on paper. An exchange of emails can lead to a contract being formed between the sender, or the school, and the recipient. Staff will never commit the school to any obligations by email or the internet without ensuring that they have the authority to do so.

Purchases for school equipment will only be permitted with permission from the headteacher, and will be purchased via the schools procurement protocols. 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 Cybersecurity procedures.

6. Portable equipment

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

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

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

Where the school provides mobile technologies, such as phones, laptops and IPads, only staff are permitted to use them.

7. Personal devices

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

Approved devices will be secured with a password or biometric access control and 2 factor authentication.

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.

During the school day, personal devices will be kept in a secure location.

8. Removable media

Only recommended removable media will be used including, but not limited to, the following:

- USB drives
- DVDs
- CDs

All removable media will be securely stored in the ICT cupboard when not in use. Staff will be required to sign removable media devices in and out when they use them.

Personal and confidential information will not be stored on any removable media.

The ICT technician will encrypt all removable media with appropriate security measures.

Removable media will be disposed of securely by the ICT technician.

9. Cloud-based storage

Data held in remote and cloud-based storage is still required to be protected in line with the UK GDPR and DPA 2018; therefore, members of staff will ensure that cloud-based data is kept confidential and no data is copied, removed or adapted.

10. Storing messages

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

If a member of staff is unsure about the correct message storage procedure, help will be sought from the ICT technician.

Employees who feel that they have cause for complaint as a result of any communications on school-owned devices will raise the matter initially with the headteacher, as appropriate. The complaint will then be raised through the grievance procedure in line with the Grievance Policy.

11. Unauthorised use

Staff will not be permitted, under any circumstances, to:

- Use the ICT facilities for commercial or financial gain without the explicit written authorisation from the headteacher.
- Physically damage ICT and communication facilities or school-owned devices.

- Relocate, take off-site, or otherwise interfere with the ICT facilities without the authorisation of the school business manager or 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 staff and Key Stage 2 users of the ICT equipment will be issued with a unique user account and password. The password will be changed every periodically. User account passwords will never be disclosed to or by anyone.
- Use the ICT equipment at any time to access, download, send, receive, view or display any of the following:
    - Any material that is illegal
    - Any message that could constitute bullying, harassment (including on the grounds of sex, race, religion/religious belief, sexual orientation or disability) or any negative comment about other persons or organisations
    - Online gambling
    - Remarks, which may adversely affect the reputation of any organisation or person, whether or not you know them to be true or false
    - Any sexually explicit content, or adult or chat-line phone numbers
- Generate messages or documents that appear to originate from someone else, or otherwise impersonate someone else.
- Install hardware or software without the consent of the ICT technician or the headteacher.
- Introduce any form of stand-alone software or removable hardware likely to cause malfunctioning of the ICT equipment 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 equipment 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 equipment without the consent of the SBM or headteacher. This is in addition to any purchasing arrangements followed according to the Manual of Internal Financial Controls.
- 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 or SBM.
- 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 equipment for personal use without the authorisation of the headteacher.
- 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 equipment.
- Be wasteful of ICT resources, particularly printer ink, toner and paper.
- Use the ICT facilities when it will interfere with their responsibilities to supervise pupils.
- Share any information or data pertaining to other staff or pupils at the school with unauthorised parties. Data will only be shared for relevant processing purposes.
- Operate equipment to record an image beneath a person's clothing with the intention of observing, or enabling another person to observe, the victim's genitals or buttocks without their knowledge or consent, whether exposed or covered by underwear – otherwise known as "upskirting".

Any unauthorised use of email or the internet will likely result in disciplinary action, including summary dismissal, in line with the Disciplinary Policy and Procedure.

If a member of staff is subjected to, or knows about harassment, upskirting or bullying that has occurred via staff email or through the use of school-owned devices, they will report this immediately to the headteacher.

12. Loaning electronic devices

School equipment, including electronic devices, will be loaned to staff members in line with a person/s role or responsibility.

Equipment and devices will only be loaned to staff members who have read, signed and returned the terms of use, as set out in the Staff Declaration Form.

By loaning school equipment and electronic devices, staff members will be agreeing to act in accordance with the terms of acceptable use.

Once a request has been authorised, the staff member will be required to undergo any training required to use the requested equipment, including how to store, handle and if applicable maintenance.

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

Staff members will be made aware that, at the discretion of the headteacher, late returns may incur a penalty fee.

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

13. Purchasing

Requests for equipment or electronic devices will be made in writing to the Headteacher via a requisition form located in the school office.

Requests will be submitted in sufficient detail for an informed decision to be made.

Requests made for equipment or electronic devices that exceed the predetermined amount allocated will require discussion and authorisation by the governing board.

Individual staff members will not be permitted to purchase equipment or devices, or process payments for such goods, on the school's behalf unless permission has been sought from the headteacher.

The cost of any equipment or devices personally purchased by staff members will not be reimbursed by the school, unless otherwise specified by the headteacher.

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

The SBM will seek advice from the ICT technician and professionals when purchasing equipment.

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

The SBM will maintain a Fixed Asset Register which will be used to record and monitor the school's assets. All equipment and electronic devices purchased using school funds will be added to this register.

When devices are not fit for purpose, or are at least ten years old, staff members may request new equipment. If their request is granted, the old equipment or electronic device will be returned to the SBM, including any accessories which were originally included with the device. Any old devices will then be disposed of or wiped clear by the ICT technician.

14. Safety and security

The school's network will be secured using firewalls in line with the Data and Cyber-security 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 the ICT technician.

Approved anti-virus software and malware protection will be used on all approved devices and will be updated termly or whenever new patches are released.

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

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

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

Members of staff who install or remove software from a school-owned electronic device without seeking authorisation from the SBM, may be subject to disciplinary measures.

All devices will be secured by a password and or 2 factor authentication.

Passwords will be kept confidential and must not be shared with pupils, unauthorised members of staff or third parties.

Devices will be configured so that they are automatically locked after being left idle for a set time.

All devices must be encrypted using a method approved by the ICT technician and Data Protection Officer.

Further security arrangements are outlined in the Data and Cyber-security recovery plan.

15. Loss, theft and damage

For the purpose of this policy, **"damage"** is defined as any fault in a school-owned electronic device caused by the following:

- Connections with other devices, e.g. connecting to printers which are not approved by the ICT technician
- Unreasonable use of force
- Abuse
- Neglect
- Alterations
- Improper installation

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

Staff members will use school-owned electronic devices within the parameters of the school's insurance cover – if a school-owned electronic device is damaged or lost outside of school hours and/or off-site, the member of staff at fault may be responsible for paying damages.

Any incident that leads to a school-owned electronic device being lost will be treated in the same way as damage.

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

The ICT technician will be contacted if a school-owned electronic device has a technical fault.

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

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

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

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

The school will accept payments made via credit and debit cards, cheque or bacs.

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

The headteacher may agree to accept the payment in instalments.

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

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

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

If a school-owned device is lost or stolen, or is suspected of having been lost or stolen, the SBM 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.

16. 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.

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

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

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

The 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.

The school's database systems are computerised. Unless permission is granted due to virtue or a person's role or responsibility, system access will be prohibited. 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 periodically or if a breach of password should occur. 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 school office administrators or system administrators and the ICT technician.

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.

17. Monitoring and review

This policy will be reviewed annually.

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

The scheduled review date for this policy will be March 2026.