Hunwick Primary School

ICT Acceptable Use Policy for Staff

Introduction

The school has provided ICT devices for use by staff as important tools for teaching, learning, and administration of the school. Use of school devices, by members of staff and visitors, is governed at all times by the following policy. Please ensure you understand your responsibilities under this policy, and direct any questions or concerns to the IT Manager in the first instance.

All members of staff have a responsibility to use the school's ICT system in a professional, lawful, and ethical manner. Deliberate abuse of the school's ICT system may result in disciplinary action (including possible termination), and civil and/or criminal liability.

The school's learning platform, provided by Google is considered as a part of the school ICT system and is therefore also covered by this policy.

Please note that use of the school network is intended to be as permissive and flexible as possible under current UK legislation and DfE guidelines. This policy is not intended to arbitrarily limit the ways in which you can use the system, but to ensure compliance with the legal responsibilities of the school and staff, to safeguard the reputation of the school, and to ensure the safety of all users. Please respect these guidelines, many of which are in place for your protection.

Lastly, the school recognises that the distinction between use of technology at work and at home is increasingly blurred, with many of us now using our own devices for work. While the school neither wishes nor intends to dictate how you use your own device, staff should consider that the spirit of this policy applies whenever you are undertaking an activity that stems from your employment with the school.

ICT Security

- You will be provided with personal accounts for accessing the ICT systems, with your own username and password. These accounts will be tailored to the level of access you require, and is for your use only. As such, you must not disclose your password to anyone including IT support staff. If you do so, you will be required to change your password immediately.
- You must adhere to the school ICT Password and Account Policy.
    - A copy of the 'ICT Password and Account Policy' should be included or stored with this document and will be available on the 'IT Support' section of the intranet or by requesting a copy from the school.
- You must not allow a pupil to have individual use of a staff account under any circumstances, for any length of time, even if supervised.
- When leaving a device unattended, you must ensure you have either logged off your account, or locked the device to prevent anyone using your account in your absence.
- You must not store any confidential, personal or special category information about staff or students on any storage system or device (such as a USB memory stick, portable hard disk, laptop, tablet or personal computer) unless that storage system is encrypted and password protected. You must also ensure that the device is securely wiped when you dispose of it.
- You must not transmit any personal or special category information about staff or students via email without the data being encrypted by a method approved by the school.
- When publishing or transmitting non-sensitive material outside of the school, you must take steps to protect the identity of pupils.
- If you use a personal device at home for work purposes, you must ensure that any school-related personal or special category information is encrypted and secured to prohibit access by any non-member of staff. School related information must not be accessible to any other person including family members and friends.
- You are responsible for maintaining a backup of data kept on any storage system other than the network storage drives, your 'My Documents' folder and the official school Google Drive. This includes tablets (iPads), USB memory sticks (even those owned or issued by the school) or a personal computer. The same rules that apply to school data also apply to backed up data. Backups must be encrypted and/or stored on an encrypted device.

- You must ensure that items of portable ICT equipment (such as laptops, tablets, digital cameras, or portable projectors) are securely stored in a locked room or cupboard when left unattended.
- You are responsible for school equipment taken off the premises. Equipment taken off the premises is not routinely insured by the school. If you take any school equipment off the premises, you should ensure that adequate insurance cover has been arranged to cover against loss, damage, or theft.
- You must not take any device capable of storing data (ie tablets, laptops and computers) out of school unless it has been encrypted and the loan has been approved by the IT Manager or Headteacher.
- You must not connect any device containing school data to any unprotected or publically accessible networks. This includes unencrypted wireless networks
- You must not remotely connect to a school IT system on any publically accessible device such as a computer in an internet café.

Data Protection

You are expected to have read the school data protection policies and have the following responsibilities

- Collecting, storing and processing any personal data in accordance with the data protection policy
- Informing the school of any changes to your personal data, such as a change of address
- Contacting the Data Protection Officer in the following circumstances:
    - With any questions about the data protection policy, data protection law, retaining personal data or keeping personal data secure
    - If you have any concerns that the data protection policy is not being followed
    - If you are unsure whether or not you have a lawful basis to use personal data in a particular way
    - If you need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a potential data breach
    - Whenever you are engaging in a new activity that may affect the privacy rights of individuals
    - If you need help with any contracts or sharing personal data with third parties

Cloud Based Services Providers

A cloud based service is a service provided by an organisation or company where data is stored electronically outside of the school. This includes all apps and websites where data is collected or shared with.

The school must adhere to data protection legislation and may be prohibited from storing data on some services because of the location, security or privacy policy.

- You must not use any unapproved cloud storage systems (Dropbox, icloud etc) for storing any school data. The only approved system for cloud data storage is the school learning platform (Google Drive). You are not permitted to use Google Drive for school data if you are using a personal account or any account not provided by the school.
- Staff must seek permission before storing any data relating to children or staff on any external website or cloud based service. This includes signing up for any website account for the children to use or entering the names or information about children on any website that has not been approved for by the school.
- The school will maintain a list of approved websites for data storage and information about how the data is stored and the steps that have been take to ensure compliance with data protection legislation.
- The school will maintain a list of cloud service providers. Staff must use or not transfer any data (including photographs) to any cloud service provider (website or app) other than those on the approved list.
- Staff must not make any agreement or sign any contract with a cloud service provider without the agreement of the Headteacher, Data Protection Officer and IT Manager. A full risk assessment of cloud service providers must be completed before any agreement is entered into.

Personal Use

The school recognises that occasional personal use of the school's ICT systems is beneficial both to the development of your IT skills and for maintaining a positive work-life balance. Such use is permitted, with the conditions that such use

- must comply with all other conditions of this AUP as they apply to non-personal use, and all other school policies regarding staff conduct;
- must not interfere in any way with your other duties or those of any other member of staff;
- must not have any undue effect on the performance of the ICT system; and
- must not be for any commercial purpose or gain unless explicitly authorised by the school.

Personal use is permitted at the discretion of the school and can be limited or revoked at any time.

Any hardware and software provided by the school for staff use can only be used by members of staff and its use must be in line with this policy.

Use of your own Equipment

- Any mains-operated personal device or electrical equipment brought on site, for any use, is subject to a Portable Appliance Test (PAT) by site maintenance staff, and must not be used until approved. This test must be performed at regular intervals as required by school's normal rules on electrical safety testing.
- You must not connect personal computer equipment to school computer equipment without prior approval from IT network staff.
- If you keep files on a personal storage device (such as a USB memory stick), including cameras, you must ensure that other computers you connect this storage device to (such as your own computers at home) have an adequate and up-to-date anti-virus system running to protect against the proliferation of harmful software onto the school ICT system.
- If you are accessing any school system (including email and cloud storage) from outside of school then you must ensure that the device that you are using has an adequate and up-to-date anti-virus system running. You must also ensure that nobody but you can access the data that you have stored accessed.
- Staff must never use phones or any device other than those owned by the school for taking photographs or videos of children.

Conduct

You must at all times conduct your ICT usage professionally, which includes being polite and using the system in a safe, legal and business appropriate manner. Among uses that are considered unacceptable are the following:

- Using, transmitting, or seeking inappropriate, offensive, pornographic, vulgar, suggestive, obscene, abusive, harassing, threatening, racist, sexist, or defamatory language or materials;
- Making ethnic, sexual-preference, or gender-related slurs or jokes.
- You must respect, and not attempt to bypass, security or access restrictions in place on the ICT system.
- You must not intentionally damage, disable, or otherwise harm the operation of devices.
- You must make efforts not to intentionally waste resources. Examples of resource wastage include:
    - Excessive downloading of material from the Internet;
    - Excessive storage of unnecessary files on the network storage areas or learning platform.
    - Unnecessary printing.
- You should avoid eating or drinking around ICT equipment.
- You must not attempt to install any purchased or downloaded software, including browser extensions and toolbars, or hardware without permission from the system manager.

Use of Social Media, Websites and Apps

Staff must take care when using social networking websites or apps such as Instagram, Facebook or Twitter, even when such use occurs in their own time using their own device. Social Networking services invite users to participate in informal ways that can leave you open to abuse, and often make little or no distinction between adult users and children.

Staff should also take care when posting to any public website (including online discussion forums or blogs) that their comments do not harm their professional standing or the reputation of the school – even if their online activities are entirely unrelated to the school.

- You should avoid allowing pupils to access personal information that you post online..
- We request that you do not identify the school as your employer on social media or any online service to reduce the possibility of unwanted contacts.
- It is essential that you do not accept any contact from current school pupils, or ex-pupils under the age of 18 on a personal account.
- You must not communicate with current pupils or ex-pupils under the age of 18 using any social media or any online service.
- You should ensure that personal information is not accessible via a 'Public' setting, but ensure it is set to a 'Friends only' level of visibility.
- You should take steps to ensure that any person contacting you via social media or any online service is who they claim to be, and not an imposter, before allowing them access to your personal information.
- You are also strongly advised not to have relatives of current pupils as friends on any social media account. You may be giving them access to your personal information and allowing them to contact you inappropriately through unregulated channels. They may also be giving you access to their personal information and activities which could cause safeguarding concerns.
- Unless authorised to do so, you must not post content on social media or any online service that may appear as if you are speaking for the school.
- You should not post any material online that can be clearly linked to the school that may damage the school's reputation.
- You should avoid publishing any material clearly identifying yourself, another member of staff, or a pupil, that could potentially be used to embarrass, harass, or defame the subject.
- When publishing content or comments on social media or any online service you are always expected to demonstrate the same level of propriety as you would while in school.

The school recognises that many staff will actively use Facebook, Twitter, and other such social networking sites, blogging and messaging services. Staff must not post material (including text or images) which damages the reputation of the school or which causes concern about their suitability to work with children. Staff must recognise that it is not appropriate to discuss issues relating to children or other members of staff via these networks. Those who post material which could be considered as inappropriate could render themselves vulnerable to criticism or allegations of misconduct.

Mobile Phones

- Staff mobile phones are allowed in school but their use must comply with the online safety policy. Staff are expected to have read the online safety policy. Mobile phones should only be used when not working with children.
- Cameras on personal phones or tablets will not be used to take pictures of children in any circumstances.
- Staff must not use their mobile phone for school business such as contacting parents.

Use of Digital Images

Any photos or videos taken by teachers, other adults (including parents), and the children themselves during any school activity (including educational visits) should not be put on public display or published anywhere on the internet (including social networking services).

The above excludes the publication of photos on the school website, within school related publicity, and where used by the school for educational / display uses.

Use of Email

All members of staff with a network account are provided with an email account for communication both internally and with other email users outside the school. The following considerations must be made when communicating by email:

- You should only use email accounts provided by the school to send emails relating to school business. Use of personal email accounts for this purpose is prohibited.
- E-mail has the same permanence and legal status as written hard copy (paper) documents and may be subject to disclosure obligations in exactly the same way. Copies of emails may therefore have to be made available to third

parties. You must be cautious when sending both internal and external mails. The professional standards that apply to internal memos and external letters must be observed for e-mail.

- Email to outside organisations has the same power to create a binding contract as hard copy documents. Check email as carefully as written contracts, always use a spell checker and, where appropriate, obtain legal advice before sending. You must not purchase goods or services on behalf of the school via email without proper authorisation.
- E-mail is not a secure method of communication, and can be easily copied, forwarded and archived. Unless explicitly authorised to do so, you must not send, transmit, or otherwise distribute proprietary information, copyrighted material or confidential information belonging to the school.
- Having an external email address may lead to receipt of unsolicited e-mail containing offensive and/or sexually explicit content. The school will take measures to minimise the receipt and impact of such content, but cannot be held responsible for material viewed or received by users from the Internet.
- You are expected to exercise caution when opening links or attachments to avoid exposing yourself or the school to potentially unwanted or damaging material, websites or malware. Do not open or click on anything that you did not expect to receive or have any doubt about.
- You must not send chain letters or unsolicited commercial e-mail (also known as SPAM).

Supervision of Pupil Use

- Pupils must be supervised at all times when using school ICT equipment. When arranging use of ICT facilities for pupils, you must ensure supervision is available.
- Supervising staff are responsible for ensuring that the separate Acceptable Use Policy for pupils is enforced.
- To avoid accidental damage to IT equipment pupils must be supervised while collecting, moving or putting away IT equipment.
- Supervising staff must ensure they have read and understand the separate e-safety policy, which pertains to the child protection issues of ICT use by pupils.

Privacy

- Use of the school ICT system, including your email account and storage areas provided for your use, may be subject to monitoring by the school to ensure compliance with school policies and applicable laws. This may include remote monitoring of an interactive logon session. In particular, the school does keep a complete record of sites visited on the Internet by both pupils and staff, however, usernames and passwords used on those sites are NOT monitored or recorded.
- You should avoid storing sensitive personal information on the school ICT system that is unrelated to school activities (such as personal passwords, photographs, or financial information).
- The school may also use measures to audit use of ICT systems for performance and diagnostic purposes.
- The school uses software that allows staff to view and take control of student devices. You should be aware that if you are using a student device then it may be possible for other members of staff to observe what you are doing. This is limited to student devices. If you are in any doubt about this then you should contact a member of the IT support staff.

Confidentiality and Copyright

- Respect the work and ownership rights of people outside the school, as well as other staff or pupils.
- You are responsible for complying with copyright law and licenses that may apply to software, files, graphics, documents, messages, and other material you wish to use, download or copy. Even if materials on the school ICT system or the internet are not marked with the copyright symbol (©), you should assume that they are protected under copyright laws unless there is an explicit permission on the materials to use them.
- You must consult a member of IT Network staff before placing any order of ICT hardware or software, or obtaining and using any software you believe to be free. This is to check that the intended use by the school is permitted under copyright law (as well as to check compatibility and discuss any other implications that the purchase may have). Do not rely on the claims of suppliers, who do not have specific knowledge of the school's systems.

- As per the standard staff contract, any invention, improvement, design, process, information, copyright work, trademark or trade name made, created or discovered by you during the course of your employment in any way affecting or relating to the business of the school or capable of being used or adapted for use within the school shall be immediately disclosed to the school and shall to the extent permitted by law belong to and be the absolute property of the school.
- By storing or creating any personal documents or files on the school ICT system, you grant the school a non-exclusive, universal, perpetual, irrevocable, and royalty-free license to use, copy, and distribute those documents or files in any way the school sees fit.

Reporting Problems with the ICT System

It is the job of the IT Manager to ensure that the school ICT system is working optimally at all times and that any faults are rectified as soon as possible. To this end:

- You should report any problems using the IT Helpdesk system as soon as is feasible. Only jobs logged using the helpdesk system will be investigated. If you feel that a problem requires an urgent response then you should ask a member of the admin staff to report the problem by telephone and report it using the helpdesk system.
- If you suspect your device has been affected by a virus or other malware, you must report this to a member of IT Network staff immediately.
- If you have lost documents or files, you should report this using the helpdesk system as soon as possible. The longer a data loss problem goes unreported, the lesser the chances of your data being recoverable (mere minutes can count).

Reporting Breaches of this Policy

All members of staff have a duty to ensure this Acceptable Use Policy is followed. You must immediately inform a member of the IT team, or the Head Teacher, of abuse of any part of the ICT system. In particular, you should report:

- any websites accessible from within school that you feel are unsuitable for staff or student consumption;
- any inappropriate content suspected to be stored on the ICT system. This may be contained in email, documents, pictures, etc;
- any breaches, or attempted breaches, of ICT security; or
- any instance of bullying or harassment suffered by you, another member of staff, or a pupil via the school ICT system.

Reports should be made either via email or the online helpdesk system. All reports will be treated confidentially.

Review and Evaluation

This policy will be reviewed regularly and in response to any changes affecting the basis of the original risk assessment, for example: significant security incidents, new vulnerabilities and significant changes to the organisation or technical infrastructure. Changes to this policy will be communicated to all staff.

Notes

Personal information is any information relating to an identified, or identifiable, individual. This may include the individual's: Name (including initials), identification number, location data, online identifier, such as a username. It may also include factors specific to the individual's physical, physiological, genetic, mental, economic or cultural or social identity.

Special Category information is personal data which is more sensitive and so needs more protection, including information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics, biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes, health – physical or mental, or sex life or sexual orientation,

Further information can be found in the school's Data Protection Policy.

Last Reviewed: 22 June 2020