The Schools of Woolton Hill

Acceptable Use of ICT

January 2023

Reviewed by Paul Davies

Approved by Governing Body: January 2023

Next Review: January 2024

Acceptable Use of ICT Policy

Aims and Purposes

To ensure that members of staff are fully aware of their professional responsibilities when using ICT and when working with pupils and parents, they are asked to sign for this code of conduct. This policy should be read in conjunction with the 'Online Safety', 'Online Learning', and 'Data Protection' policies, as well as the Pupil Privacy Notice and Staff Privacy Notice.

Systems and Permissions

- I appreciate that ICT includes a wide range of systems, including laptops, tablets, mobile phones, PDAs, digital cameras, email and social networking.

- I know that personal equipment may not be brought onto site and used to replace school items. If something is broken, the IT coordinator will endeavour to resolve the issue in good time. Electronic devices may only be brought in with specific permission from the IT coordinator and caretaker, and must be PAT tested before use.

- I understand that access to certain software packages and systems (e.g HCC intranet; SAP (HR, finance and procurement system), ARBOR, RAISE Online, FFT, school texting services) will be restricted to nominated staff and unless permission and access has been provided, staff must not access these systems.

- I understand that I must not use the school ICT system to access inappropriate content at any time. This includes obscene and indecent images, blocked websites (of an adult/mature content, e.g. gambling, betting, gaming, alcohol, tobacco, illegal drugs, auction sites, radicalisation and terrorism, promotion of gang culture or violence).

- I understand that school information systems and hardware (including laptops, iPads issued to staff, cameras and equipment) may not be used for personal purposes without specific permission from the head teacher. I understand that it is my responsibility to look after, keep safe and respect the equipment I have been personally issued, and that I may need to contribute financially to a replacement if this is not deemed to be the case. In addition, we all have collective responsibility for shared items such as laptop trolleys and their contents. Year groups or individual children may receive a ban for inappropriate use or for damaging any shared equipment intentionally. Where appropriate, a child's parents may be contacted and a financial contribution to a replacement device requested.

- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance. The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound. This includes connecting to the school Wi-Fi system for personal use on mobile phones. In cases where allegations of improper conduct have been made, police involvement may be necessary.

- I will not install any software or hardware from any source without permission.

- I will respect copyright and intellectual property rights.

- I understand use for personal financial gain, gambling, political activity, advertising, commercial ventures, personal campaigns or illegal purposes is not permitted.

- I will ensure that I use the school email account I have been provided with solely for the purpose of carrying out my job effectively. I will not use it to communicate with parents or pupils, unless an appropriate colleague/member of SLT has been copied in (CC'd). My personal e-mail accounts must never be used to conduct school business. The only exception to this is LinkedIn (or other professional networks), where it is acceptable to use an e-mail account that covers both professional and personal use. The office staff reserves the right to access employee's school e-mail accounts if it is anticipated that important communications may be missed due to absence.

Teaching and Working with Pupils

- I will not use my mobile phone or hands-free device whilst driving on school business. I understand that I may use my personal mobile phone in exceptional circumstances, such as to contact the school whilst on an off-site visit. I will never use my mobile phone or tablet to take photos of children.
- I will ensure I check the content of any video, photo or audio clips I intend to use with children in advance. I must deem it appropriate before use in the classroom. I will disable the autoplay function when watching educational YouTube videos in school.
- I will report any incidents of concern regarding children's safety to the schools Online Safety Coordinator, the Designated Safeguarding Leads or Head teacher, using CPOMS and categorising the incident as an online safety concern. I will ensure that I verbally contact any member of staff necessary in urgent cases.
- I understand the recent development in the use of online platforms to promote radicalism and extremism to wider audiences, and that I must report any concerns of this nature using CPOMS, or if urgent/extreme in nature, contact a DSL immediately.
- I will promote and model online safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing. See Online Safety policy and Purple Mash Curriculum for more details.

Personal Use of ICT

- I will make appropriate use of the security settings available on social networking sites and ensure these are updated as the sites make changes themselves. With increasing concerns over identity theft and fraud, I will consider how much personal data is held about me on profiles.

- Only administrative staff and management may use social networking sites as a means of communicating with the school community.

- I will contact a member of the management team if I have any concerns over the safety or security of pupils, staff, parents, equipment or information.

- I understand that the school has an iCloud account which can be used, in consultation with the head teacher and IT co-ordinator, to purchase songs, apps and films. I will not log into my personal iCloud account to download such items, even if this is for an educational purpose. Apps may only be downloaded on iPads with permission and by the IT coordinator.

- I will not access my mobile phone during lessons unless I am either reading/writing emails or adding information to CPOMS. I may also keep my phone with me if I am expecting an important personal call that cannot be avoided.

- I will not share any inappropriate personal photos or videos with children in my care.

Social Media

It is recognised that social networking has the potential to play an important part in many aspects of school life, but staff members must be conscious at all times of the need to keep their personal and professional lives separate. The Schools of Woolton Hill respects your right to a private life but has a duty to provide a safe working environment for all stakeholders. This policy applies to personal webspace, such as social networking sites, blogs, microblogs including Twitter, chat rooms and podcasts and content sharing sites such a Flickr and YouTube.

- I understand the need to exercise extreme care in my personal use of social networking sites. I know that inappropriate communications that come to the attention of school can lead to disciplinary action, including dismissal.

- I will ensure I do not have any pupils or ex-pupils under the age of 18 as friends on social networking sites, including former pupils, and those who have moved to other schools. I will not have any unauthorised contact (electronic) with pupils, current or past, outside of school hours.

- I must not post photos that include any background details that could be used to identify the school, its systems, or stakeholders.

- I will not reference pupils, students or parents in posts without their approval.

- I will exercise caution when having contact with, or accepting friend requests from parents.

- I will ensure my comments and posts will not compromise the school's reputation, credibility, information, computer systems or networks. This includes openly identifying themselves as school personnel and making disparaging remarks about the school, its' policies, other staff members and other people associated with the school. I will not express personal views online that the school would not want to be associated with.

- I know that my comments, posts and online activity should not breach any of the policies I have read and signed.

- I will ensure my comments and posts must not be of an illegal, sexual, discriminatory, offensive, hateful, threatening or abusive nature.

- The tone of my comments and posts must not damage relationships with work colleagues in the school, partner organisations, pupils or parents.

- I understand that any harassment of other staff via social media will be investigated by the Senior Leadership Team and may lead to disciplinary action. This includes when the person being targeted is unaware of the comments and posts being made. It is everyone's responsibility to report any such behaviour to either the Computing coordinator or Senior Leadership Team. It is advised that anyone wishing to report or discuss alleged incidents keep screen-shots, e-mails, text messages or phone logs as evidence. Do not delete any such material. If the concern is in regard to the conduct of the head teacher, this must be disclosed to the chair of governors.

GDPR

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner. I will ensure that, when taken home for work use, my laptop and other equipment cannot be accessed by others. If staying logged into work e-mails on my own personal devices, I must ensure only I know the passcode. I will consider using fingerprint recognition options if they are available to me.

- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager. I will not use anyone's account except my own. I will not distribute or share personal details of others – in line with the school's Data Protection Policy. When using a shared computer, I will ensure I sign out of websites/programs to ensure data is not misused or accessed without permission.

- I will ensure that sensitive personal data is stored securely and is used appropriately, whether in school or accessed remotely. It must NOT be kept on removable storage devices, taken off premises or kept in cloud storage, e.g. Dropbox, Google Drive and iCloud.

- Any photos of children taken using the school's digital cameras or other equipment must be kept secure and safe. The school has a networked server which can be used to store the images. They must be deleted at the end of every academic year.

I have read, understand and accept the staff code of conduct regarding the Acceptable Use of ICT.

Appendix – Remote Working Guidance

APPENDIX to AUP

REMOTE WORKING GUIDANCE

We have prepared this remote working guidance to assist the school in managing staff who are working from home as organisations have had to adapt how staff perform their roles during lockdown.

This guidance is aimed primarily at the school Data Protection Officer who is likely to be involved with ensuring that these issues have been considered. When considering this you should also review whether data protection e-learning for staff is up to date. If there is a reportable breach caused by home working one of the first questions the ICO will ask is when the staff last completed their DP training. Any guidance provided to staff on working from home would provide some evidence of measures taken by the school to mitigate any risks posed by home.

Follow the school's policies, procedures, and guidance.

The school has guidance and policies and procedures in place to help you remain compliant while working from home. These policies include, but are not limited to,: AUP and Online Safety and are available on the server.

If you have any concerns about working from home then contact the school's Data Protection Officer as soon as possible to discuss matters

Only use approved technology for handling personal data

If you have access to a device issued by the school, use it. This will help keep the data you are accessing secure. Keep the device secure by following the school's password requirements.

If you are considering working from home using your own computer or laptop then this should be approved by the school. You may be asked to implement further security requirements on your home machine.

The school ***does not*** approve the use of USB memory sticks, encrypted or otherwise.

We recommend that any decision to depart from the approved school technology should be discussed with, and be documented by, the DPO.

Consider confidentiality when holding conversations or using a screen.

If you have a conference call, video call, meeting or phone call when working from home, be careful about what you say and where you say it. Think about whether you can be overheard, for example if you are working in your garden or with windows and doors open. Find places in your home where you can have confidential conversations, if possible.

Consider the security of your working from home setup. Try to keep your screen from being visible to other members of your household and lock your screen (Windows Key + L) when it is not in use.
It will be your responsibility to keep the school's information secure at home.

Take care with print outs.

Avoid printing out any confidential data, such as the personal data of pupils, if possible - view this information on the screen of your device. If you have to print out confidential information, store any paperwork in a locked cupboard, drawer, bag, or briefcase. Avoid disposing of or shredding paperwork at home. Store it securely and return it to the school for secure disposal when you are able.

Lock it away where possible.

To avoid unauthorised access, loss or theft of personal data you should put away and, if you can, lock up paperwork and devices (i.e. hybrids, laptops) at the end of the working day (and when not in use for extended periods).

Keep all work documents separate from personal documents.

Hold information under lock and key when not in use, e.g. in a locked bag, briefcase, drawer, or cupboard. If possible, store paperwork in a separate bag from IT equipment.

If you are travelling by car and stop off anywhere while transporting information, consider whether it is safer to leave files or devices securely locked and out of sight in the boot of the car or to take them with you.

Never leave information or your devices in a car overnight – keep it inside your home.

Take home only the paperwork required and return it to the school as soon as is practicable

Be extra vigilant about opening web links and attachments in emails or other messages.

Cyber criminals are preying on fears of the coronavirus and sending 'phishing' emails that try and trick users into clicking on a bad link. Once clicked, the user is sent to the criminals' website, which could download malware or virus onto your computer or steal passwords.

The scams may claim to have a 'cure' for the virus, offer a financial reward, or be encouraging you to donate.

If you receive a suspicious email, do not open any attachments, click on links or immediately delete it. Flag it up as an IT security threat in accordance with the school's procedures and follow any advice on the next steps to take.

Communicate securely.

If you are sending information by email do not use a personal email address or social media or file sharing account to send school information that includes personal details.

Keep software up to date.

Please ensure that you bring in school issued equipment regularly (at least once per term) and log onto the network to allow any updates to download.

If you are using your own equipment, don't be an easy target for hackers. Check for and install updates regularly, as this will keep your system secure and make it more difficult for them to get in.

Take care of your own focus and mental health

Data incidents are generally caused by administrative mistakes that could happen to anyone. These are often the result of being distracted, stressed or tired.

Take extra time to double-check your work (especially email addresses and attachments) to ensure that information you are sharing is going to the correct place.

Concentrate on one task at a time, dealing with particularly sensitive information in the quietest part of the day. Taking regular breaks may help improve your focus and prevent mistakes.

Report any potential data incidents.

If you identify any potential loss, unauthorised access, or misuse of personal data, report this as soon as possible to the Data Protection Officer. If possible, recover any lost information.

All reported incidents will be investigated appropriately by the DPO and steps taken to prevent any future errors.