Hampstead Hill School

Respect. Kindness. Community. Curiosity. Conservation.

Acceptable Use Policy: Staff

Table of Contents

Hampstead Hill School

Respect. Kindness. Community. Curiosity. Conservation.

1. Importance of Safe Technology Use

Technology is now entwined in our modern lives with everyday use of social media and web-based communication as standard practice. It is therefore important to ensure good awareness of the possibilities to learn, create and share ideas and also the risks that these freedoms bring, both to the welfare of staff and students and to the integrity of the IT systems that the school relies on to provide learning and teaching.

All users who access our school systems should are entitled to safe access to the internet and IT systems at all times. This policy is intended to provide a working framework for staff to uphold the positive ideals of the technology we use while providing a safe learning environment and protecting the data we manage in the course of our services to students and their families.

2. Legislation and Guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The General Data Protection Regulation
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- Keeping Children Safe in Education
- Searching, screening and confiscation: advice for schools
- National Cyber Security Centre (NCSC)
- Education and Training (Welfare of Children Act) 2021

3. Definitions

- **IT facilities:** includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the IT service
- **Users:** anyone authorised by the school to use the IT facilities, including governors, staff, pupils, volunteers, contractors and visitors
- **Personal use:** any use or activity not directly related to the users' employment, study or purpose
- **Authorised personnel:** employees authorised by the school to perform systems administration and/or monitoring of the IT facilities

- **Materials:** files and data created using the IT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

4. Outline of Policy

- Staff must ensure they are responsible users of the IT systems provided and that they make sound judgements while using the internet and other communication technologies for educational and personal use.
- The school IT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Staff can ensure they are protected from potential risk in their use of technology for educational and personal use.

5. Safeguarding and Security

- I understand that the school will monitor my use of the school IT and communication systems.
- I understand the rules in this document apply equally to the use of school and personal devices and systems (e.g. laptops, email, iPads etc.) outside of school
- I understand the importance of appropriate controls on the transfer and sharing of personal data (digital or paper-based) out of school.
- I understand that the school IT systems are primarily intended for educational use.
- I will never disclose my username or password to anyone else, nor use any other person's username and password to access systems not provided to me.
- I understand that I should not record any password where it is possible that someone may view it or steal it.
- I will immediately report any incident or activity I am aware of which may be illegal, inappropriate or present risk to the school or individuals to the IT Manager of HHS

6. Professional Use of School Technology

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Principal.
- I will communicate with others in a professional manner and refrain from any use of aggressive or inappropriate language.
- I will not engage in any online activity that may compromise my professional integrity or provide a risk to the students, my colleagues, the school IT systems or myself.
- I will not access, copy, alter, share or delete any other user's files, without their express permission.
- I will only use school provided and managed equipment unless I have explicit permission to do otherwise.
- I will ensure that any published photos do not identify individuals by name or show other personal information and that photos and images are only used on a school approved and controlled platform.
- I will only communicate with students and parents/carers using provided school IT systems. All communication will be professional in tone and manner

Hampstead Hill School

Respect. Kindness. Community. Curiosity. Conservation.

- I will not reveal my password(s) to anyone.
- I will ensure that I do not share my personal contact information and only ever use contact details provided by the school.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will report it to the IT Manager. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email /One Drive / network, or other school / Local Authority Systems.
- I will not give out my own personal details, such as mobile phone number, personal e-mail address, personal Twitter account, or any other social media link, to pupils/parents.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system(s) for any school business. (This is currently: your name or classname@hampsteadhillscool.co.uk)
- I will only use the approved school email, school Learning Platform or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will ensure that emails and other written communications are carefully and politely written.
- I will ensure that personal data (such as data held on iSAMS or CPOMS software, One Drive & all the data on the laptops) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely in a suitable environment, when authorised by one of the School Directors or the IT Manager. Personal or sensitive data taken off site must be encrypted, eg on a password secured laptop with encryption.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate IT manager.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not download executable files or unapproved system utilities as these will not be allowed, and all files held on the school ICT system will be checked regularly.
- I will not publish or distribute work that is protected by copyright.
- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role and do not bring the school's name into disrepute.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.

- I will access school resources remotely (such as from home) only through the school approved methods and interact with those materials.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will alert the school's named designated safeguarding lead / relevant senior member of staff if I feel the behaviour of any pupil I teach may be a cause for concern.
- I will only use school systems in accordance with any school policies.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.
- I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to a senior member of staff (the SMT) or the designated safeguarding lead at the school.
- I understand that failure to comply with this agreement could lead to disciplinary action.
- I will not use personal electronic devices (including smart watches) in public areas of the school between the hours of 7.45am and 5.30pm, except in the staff room and where there are signs to indicate this.
- I understand that this forms part of the terms and conditions set out in my contract of employment

7. Staff Responsibilities

- Staff must remain vigilant when accessing emails - never click on any hyperlinks in emails or any attachments to emails, unless the sender is known and trusted.
- Staff having any concerns about emails or communication received on any other school or personal IT system must report them to the IT Manager
- Staff must store all professional work in the appropriate, provided, locations on the school network or systems to guarantee appropriate levels of backup and malware scanning.
- Staff should not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.
- Staff should not install any applications on school devices without consultation and support from the IT Manager. Neither should they change settings put in place by the school to ensure appropriately managed devices.
- Staff should report any damage or faults in school equipment to the IT Manager.
- Staff must ensure that online resources are only used or shared where permission has been given by the author. Any copyrighted work will not be downloaded or shared including music and videos.

7.1 Access to school IT facilities and materials

The school's Data Manager manages access to the school's IT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets, mobile phones and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the school's IT facilities.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the Data Manager.

7.2 Use of phones and email

Mobile phones are only permitted in the Staff room or offsite. However, we acknowledge that to use two-factor authentication to access CPOMS, our platform for reporting concerns or incidents, Staff may need to use their mobile phones. Staff should ensure they do this in the Staff rooms whenever possible, however, there may be situations in which Staff cannot leave the classroom. Staff may use their mobile phones, solely for the CPOMS two-factor authentication, if there is another Staff member in the room supervising the responsible phone use.

- The school provides each member of staff with an email address.
- This email account should be used for work purposes only.
- All work-related business should be conducted using the email address the school has provided.
- Staff must not share their personal email addresses with parents and pupils and must not send any work-related materials using their personal email account.
- Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.
- Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.
- Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.
- If staff receive an email in error, the sender should be informed, and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.
- If staff send an email in error that contains the personal information of another person, they must inform the Data Manager immediately and follow our data breach procedure.
- Staff must not give their personal phone numbers to parents or pupils. Staff must use phones provided by the school to conduct all work-related business.
- School phones must not be used for personal matters.

- Staff who are provided with mobile phones as equipment for their role must abide by the same rules for IT acceptable use

7.3 Personal use

Staff are not permitted to use school IT facilities and devices for personal use.

Staff may not use the school's IT facilities to store personal non-work-related information or materials (such as music, videos or photos).

Staff should take care to follow the school's guidelines on social media and use of email to protect themselves online and avoid compromising their professional integrity.

7.4 Monitoring of school network and facilities

- The school reserves the right to monitor the use of its IT facilities and network. This includes, but is not limited to, monitoring of:
    - Internet sites visited
    - Bandwidth usage
    - Email accounts
    - Telephone calls
    - User activity/access logs
    - Any other electronic communications
- Only authorised IT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.
- The school monitors IT use in order to:
    - Obtain information related to school business
    - Investigate compliance with school policies, procedures and standards
    - Ensure effective school and IT operation
    - Conduct training or quality control exercises
    - Prevent or detect crime
    - Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

7.5 Search and deletion

- Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation.
- The school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the school's rules.
- Staff members may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse contains an online element.

8. Remote Education

Technology use should be consistent with the school's ethos, other appropriate polices and the law.

- Remote learning will only take place using the school's agreed learning platforms.
- Staff will use school equipment.
- Online contact with learners and parents/carers will take place at agreed times as set out in the timetables.
- All remote teaching, and any other online communication, will take place in line with current school confidentiality expectations as outlined in HHS' model safeguarding policy and KCSiE (2020).
- Access to the school's approved learning platform(s) will be restricted to staff, pupils and parents.
- Pupil and staff access to the learning platform will be managed in line with current IT expectations as outlined in this policy.
- Staff will record pupils' attendance daily
- The use of educational resources will be in line with existing HHS practices, with consideration made to licensing and copyright.
- Staff will model good practice and moderate behaviour online during remote sessions, as they would in the classroom.
- All participants are expected to behave in line with existing school policies and staff will remind pupils of behaviour expectations as and when appropriate.
- Inappropriate behaviour will be addressed in line with the school behaviour and remote learning policies.
- When delivering live or pre-recorded lessons, staff will:
    - Wear appropriate dress
    - Not take or record images for personal use
    - Ensure that personal information and/or unsuitable personal items are not visible, either on screen or in video backgrounds
    - Ensure all sensitive documents or tabs are closed when screen sharing
    - Make suitable arrangements to ensure privacy and avoid unnecessary intrusion

Staff are encouraged to report concerns about remote and/or live-streamed sessions through appropriate school procedures – to the IT Manager or the Safeguarding Team depending on the nature of the concerns.

9. Links with Other Policies and Documents

- Safeguarding and Child Protection Policy
- Behaviour Policy
- Data Protection Policy
- Privacy Notice
- Online Safety Policy
- Work out of School Policy

Last Review	January 2024
Next Review	January 2025

Hampstead Hill School

Respect. Kindness. Community. Curiosity. Conservation.

Name	 Anne Napier Headteacher