Perrott Hill School

Staff Acceptable Use Policy

Technologies, Internet & Computers

The Board of Directors has charged the Proprietor with day-to-day responsibility for the governance of the School. Ultimate responsibility for the governance of the School rests individually and collectively with Board of Directors.

The Proprietor chairs a Board of Governors acting in an advisory capacity in support of good governance.

SECTION ONE

PURPOSE

A. To allow for appropriate and reasonable use of electronic media and services, including computers, e-mail, on-line services, the School network, the internet and hand-held devices by the School's employees.

B. To encourage the creative and safe use of these media and associated services through clear but proportionate guidelines so as to benefit the School, pupils' learning, staff's teaching and residents' home lives. All employees and everyone connected with the School should remember that electronic media and services provided by the School are School property and their primary purpose is to facilitate and support School business. All users have the responsibility to use these resources in a professional, ethical and lawful manner. This policy covers all individuals working at all levels including casual and supply staff and volunteers.

C. To ensure that all employees are responsible, the following guidelines have been established for using technology, computers, e-mail and the internet. This policy does not cover every possible situation. Instead, it is designed to

express the philosophy of the School and set forth general principles when using electronic media and services.

D. To protect the member of staff. This staff AUP forms part of the School's 'Staff Code of Conduct' and must be read in conjunction with such.

SECTION TWO

INTERNET

Access to the internet is an integral part of staff roles at Perrott Hill and as such a higher level of internet access must be given to staff to ensure they are able to work effectively and efficiently. Staff internet access is filtered to reduce any inappropriate sites being visited. Staff must still be vigilant in what they are accessing on the internet and must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting or having links to extremist groups; promoting illegal acts; any other information which may be illegal or offensive to colleagues.

If a member of staff inadvertently accesses any website or internet service that could be classed as inappropriate, they should report it to the ICT Systems Manager immediately so future access can be restricted.

SECTION THREE

PROHIBITED COMMUNICATIONS

Electronic media must not be used for transmitting, retrieving or storing any communication that is:

- Discriminatory or harassing.
- Derogatory to any individual or group.
- Obscene, sexually explicit or pornographic.
- Defamatory or threatening.
- In violation of any licence governing the use of software.
- Engaged in for any purpose that is illegal or contrary to the school policy or interests.

The full context of the 'Staff Code of Conduct' is transferable to this user agreement with regards to conduct online and/or using School electronic devices.

SECTION FOUR

PERSONAL USE

The computers, electronic media and services provided by the School are primarily for educational use to assist employees in the performance of their jobs. Limited, occasional or incidental use of electronic media (sending or receiving), the internet or the computers for personal purposes is understandable and acceptable, and all such use should be done in a manner that does not adversely affect the systems' use for their educational purposes. However, employees are expected to demonstrate a sense of responsibility and not to abuse this privilege.

The presence of resident staff for whom the School is also their home adds its own dynamic to the use of the School's internet connection and, as far as is reasonable, it is the School's desire for resident staff to be able to use their internet connection as they would a standard domestic connection. The standards of conduct referenced in Section 2, however, clearly apply at all times. For further details on resident staff, see Section 13 below.

The School has the ability to check all usage history of its internet connection and network, but will not do so unless it feels there is a particular need to do so. (See Section 6 below.)

Personal computers and mobile devices (including mobile phones) must have a password and must not be left unlocked when unattended.

SECTION FIVE

ACCESSING SCHOOL WI-FI AND THE SCHOOL NETWORK

A. Only devices that have been checked by the ICT Department are authorised to be used to connect to the School Wi-Fi (PHS WiFi) and the hard wired network via the ports around the school campus. Any device that connects to the School network via Wi-Fi or a wired connection should have the latest updates including security patches and have valid and up to date Anti-Virus software installed.

B. There is a Wi-Fi called 'PHS Staff' which gives you access to the internet (it is independent of the School network) and can be accessed by all devices, including tablets, mobile phones and laptops that have not been checked by the ICT Department. Any device that connects to this network should have the latest updates including, firmware, OS updates, security patches and have

valid and up to date Anti-Virus software installed Details of how to access the 'PHS Staff' network are located on the staffroom notice board.

C. Visitors to the School must not connect their devices to the school network but may use the 'Visitors' Wi-Fi provided.

SECTION SIX

REMOVEABLE DEVICES; USB STICKS, SD CARDS, EXTERNAL HARD DRIVES AND STORAGE DEVICES

i) Removable devices such as USB sticks, SD cards and external Hard Disk drives may not be connected to the School network. Some sensible precautions, however, should be followed: if you suspect the device to be damaged, to contain inappropriate material or a virus, do not connect it to any School device including computers, photocopiers, laptops, tablets, cameras and phones. Give the device to the ICT Department at the earliest opportunity who will safely check and approve its use with School equipment if appropriate.

ii) No personal sensitive information (as identified in the Data Protection Act 2018 / GDPR) should be loaded onto a removable device as the information could be lost, modified or be disclosed to unauthorised personnel. If sensitive information is required to be loaded onto a removable device, encryption to a recommended standard (AES-256) must be used. The ICT Department can assist with encrypting information.

Any loss of sensitive data must be reported to the Head immediately so appropriate action can be taken.

SECTION SEVEN

ACCESS TO EMPLOYEE COMMUNICATIONS

A. Generally, electronic information created and/or communicated by an employee using e-mail, word processing, utility programs, spreadsheets, internet and bulletin board system access, and similar electronic media is not reviewed by the School. However, the following points should be noted:

The School routinely gathers logs for most electronic activities and monitors employee communications directly, e.g. internet logs, space on server, integrity of files or for the following purposes:

1. Resource allocation.

2. Optimum technical management of information resources.

3. Continuity of operational functions during personnel changes.

3. Detecting patterns of use that indicate employees are violating School policies or engaging in illegal activity.

B. The School reserves the right, at its discretion, to review any employee's electronic files and messages to the extent necessary to ensure electronic media and services are being used in compliance with the law, this policy and other School policies, or to assist in the investigation of wrongful acts, or to comply with any legal obligations of the School in its role as employer or generally.

C. Employees should not assume electronic communications or electronic files are completely private. Accordingly, if they have sensitive information to transmit, they should use other means. Employees should be aware that their school email address is the property of the school should be used for professional purposes only.

SECTION EIGHT

SOFTWARE

To ensure that the School is compliant with software licensing and to prevent computer viruses from being transmitted through the School's computer system, unauthorised downloading of any software is strictly prohibited. Any software requirements can be discussed with the ICT Department who will authorise the software installation or organise the purchasing of software licenses where applicable.

Employees should use anti-virus software on any home computer or laptop that is used to access the School network or to download lesson planning or other information onto the School computers. Employees should contact the ICT Systems and Development Manager if they have any questions or require help/advice.

SECTION NINE

SECURITY/APPROPRIATE USE

A. Employees must respect the confidentiality of other individuals' electronic communications, with the exception of cases in which explicit authorisation

has been granted by School management. Employees are prohibited from engaging in, or attempting to engage in:

1. Monitoring or intercepting the files or electronic communications of other employees or third parties.

2. Hacking or obtaining access to systems or accounts they are not authorised to use.

3. Using other people's log-ins or passwords.

4. Breaching, testing or monitoring computer or network security measures.

B. No e-mail or other electronic communications may be sent that attempt to hide the identity of the sender or represent the sender as someone else.

C. Electronic media and services should not be used in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system.

D. Anyone obtaining electronic access to other companies' or individuals' materials must respect all copyrights and cannot copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner.

E. Anyone receiving inappropriate contact from parents, past parents, pupils or past pupils should inform the Head immediately.

SECTION TEN

PARTICIPATION IN ONLINE FORUMS

A. Employees should remember that any messages or information sent on School-provided facilities to one or more individuals via an electronic network—for example internet mailing lists, bulletin boards and online services—are statements identifiable and attributable to the School.

B. The School recognizes that participation in some forums might be important to the performance of an employee's job. For instance, an employee might find the answer to a technical problem by consulting members of a news group devoted to the technical area.

SOCIAL NETWORKING SITES

Please see the separate Social Media Policy that covers all aspects of Social Media and should be followed by all members of staff (employees) and is recommended as best practice for volunteers.

If staff wish to access social networking sites whilst at work, then this must only be done as part of a reasonable 'break' and preferably on their own personal computer or mobile device (when not directly in charge of pupils) Staff should, however, remember that anything beyond light usage in the working day would be inappropriate and suggestive that aspects of their professional responsibilities were receiving less attention as a result.

When staff are using social networking, it is important to:
- observe the Social Media Policy and other School policies, particularly the 'Staff Code of Conduct' and any others with respect to confidentiality, safeguarding, professional boundaries and data protection as well as take action to protect themselves and their reputations.

Advice on this is as follows:

- Make sure that you have set the privacy and security settings to 'friends' and not 'everyone' or 'friends of friends'.
- Carefully manage your settings to ensure that mutual 'friends' or 'friends of friends' cannot gain access to your profile thus making it potentially accessible to current or past pupils/parents.
- Avoid adding students or past students and it is best practice not to add parents.
- Maintain professional standards at all times.
- Never write/post or upload images that could be interpreted as unprofessional.
- Do not directly post information about the School, pupils, past pupils, pupils' families or members of staff (past or present), including photographs.
- If you have "sensitive pictures" on your social networking site, make sure you delete them from your account. Be aware that even if you do this, they can still be found as you cannot delete your digital footprint or people may have already copied them.
- If a parent, past-parent, pupil or past pupil contacts you inappropriately or you have concerns, you must inform the Head immediately.

SECTION ELEVEN

PERSONAL DEVICES INCLUDING MOBILE PHONE USAGE

The school recognises that personal devices are a useful tool for communication and welcomes staff to use the school WhatsApp groups for school related communications, to access their school emails when they are away from their desk and to be contactable around the school campus or whilst they are off site when on school business.
Staff should use good practice and common sense when using their personal devices throughout the school day and where ever possible, staff should not use their personal devices while they are directly in charge of pupils. However, in a case of emergency such as but not limited to, a medical emergency, a lockdown procedure or extremely urgent School business, staff are allowed to use their personal devices when directly in charge of pupils but only when it is safe to do so. .

Whenever possible, staff should use a school owned device to photograph, film or record (sound and visual) pupils. However sometimes this may not be possible and a personal device is required to capture an unplanned moment or event. If this happens, as soon as feasibly possible, staff should transfer the photograph, film or sound to either the school system (such as the school network, a school Teams or a school One drive account), a school device or a school email account. Once transferred the original capture must be removed from the personal device making sure that it is permanently removed and not kept in a form of recycle bin or saved / backed up to cloud storage. Personal devices should not be used to photograph, film or record (sound and visual) pupils by anyone in the capacity of a volunteer or temporary member of staff.

Personal devices should not be used to phone pupils' personal mobile phones or contact pupils directly. If you need to speak to a pupil, then you must phone the pupil's parents and gain access to them via their parent or parents.

All devices (personal or work) must be locked with a password.

No devices (personal or work) must be used to send offensive messages or to access inappropriate websites or pictures.

When running School residential trips or any other School trips, please discuss with the Bursar (at least two weeks prior to the trip) the use of a School device.

PHOTOGRAPHY AND FILMING

All staff and volunteers whilst in the capacity of a member of staff are given guidance on the School's policy on taking, using and storing images of children. This includes:

- Staff should only use School cameras/recording devices and not personal equipment where ever possible*.
- Digital images of children must be stored on password protected School systems. .
- Digital images of pupils should not be stored on personal/home computers/hard drives.
- Hard copies of pupils' images should be stored in a locked filing cabinet on the School premises.

*Staff working with children in the EYFS must not use personal recording equipment at any time.

Please speak to the ICT Department or School Office who can loan you suitable School equipment.

Do not download any photographs, film or sound recordings of pupils onto you own personal technology, for example a workstation or laptop.

Residential trips will have access to a School laptop to e-mail photographs etc. back to School; please contact the ICT Systems and Development Manager for further information.

SECTION TWELVE

VIOLATIONS

Any employee who abuses the privilege of their access to the School network, e-mail, the internet or other technologies in violation of this policy will be subject to disciplinary action, up to and including possible termination of employment, legal action and criminal liability.

SECTION THIRTEEN

EQUIPMENT SECURITY AND PASSWORDS

Staff are responsible for the security of the computers, devices and other equipment the School allocates to them to use and must not allow such equipment to be used by anyone other than in accordance with this policy.

Passwords are for the benefit of the School, are the confidential property of the School and must be used to secure access to data kept on such equipment, thereby ensuring that confidential data is protected in the event of loss or theft. Passwords must not be made available to anyone else unless authorised by the ICT Department.

If you feel that someone else knows your password or that your account has become compromised in any way, please change your password immediately and inform the ICT Department of this concern straight away.
The system is set for your password to change periodically and will request you to change your password once it has expired. However, passwords must be changed every term and it is the responsibility of the user to change their password even if they haven't been asked to change their password automatically. Passwords must be a complex combination of upper and lower case characters, numbers and other symbols such as @, #,! etc. It is also good practice not to use words found in a dictionary or something easily associated with the user such as a family member's name, address, pets name etc.
Staff need to take caution on any request via email or other electronic communication that immediately requires them to provide security information such as a password or answers to security questions. All Microsoft related systems have Perrott Hill branding so if you are ever asked to enter your school email address and password, please ensure that the password screen has Perrott Hill branding and looks authentic. If not or you have any doubt, do not enter in your details and contact the ICT department for further assistance.

SECTION FOURTEEN

RESIDENT STAFF

Most of the School's residential accommodation have access to the 'Residential' WiFi network which is unfiltered, but are monitored in line with safeguarding requirments.

Whilst using the School's computer system from residential accommodation, any illegal activity such as downloading of copyrighted material such as music, films and computer games, accessing illegal material on the internet etc. is strictly forbidden and will result in disciplinary action and will be reported to the Police.

Staff discretion in line with all of the guidance above is advised when accessing the internet from residential accommodation and any inappropriate usage may result in disciplinary action.

SECTION FIFTEEN

PERSONNEL RESPONSIBLE FOR THE POLICY

The Head has overall responsibility for the effective operation of this policy but has delegated day–to-day responsibility for its operation to the ICT Systems and Development Manager (Lee Andrews). Unless otherwise stated, any request for any permission, authority, assistance or advice under any provision of this policy should be made to the ICT Systems and Development Manager.

Staff are invited to direct any comments and suggested improvements to this policy document to the ICT Systems and Development Manager.

SECTION SIXTEEN

EMPLOYEE AGREEMENT ON USE OF SCHOOL SYSTEMS, E-MAIL, THE INTERNET AND TECHNOLOGIES.

By using the systems of PHS I accept that I have read, understand and agree to comply with the Staff Acceptable Use Policy, rules and conditions governing the use of Perrott Hill School's systems, computers, networks, internet and telecommunications equipment and services. I understand that this includes the use of my personal devices. I understand that I have no expectation of privacy when using telecommunications equipment or services whilst at the School or on School trips and business. I am aware that violations on the areas covered in this policy may subject me to disciplinary action, up to and including termination of employment, legal action and criminal liability. I further understand that my use of my personal or school electronic communication or social media posts may reflect on the public image of Perrott Hill School and that I have responsibility to maintain a positive representation of the School. Furthermore, I understand that this policy can be amended at any time and that the IT Systems and Development Manager will notify me of any changes.