Perrott Hill School

Staff Acceptable Use Policy

Technologies, Internet & Computers

Day-to-day responsibility for the governance of the school lies with the Board of Governors whilst the Chair of the Board of Directors holds ultimate responsibility.

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 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 and network. 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. 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 Wi-Fi 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 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 (1988)) 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. 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.

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

The following should be followed by members of staff (employees) and is recommended as best practice for volunteers.

Social networking sites, such as Facebook, YouTube or Twitter, are very much part of the age in which we now live, but they are not without their perils and staff must be aware of this to avoid possible significant professional problems.

Staff must not access social networking sites whilst teaching a lesson or when directly in charge of pupils.

Staff are role models for their pupils and their conduct should be beyond reproach. Therefore, staff must not include pupils or past pupils within their 'social networking' as this can be misinterpreted and can lead to career-threatening allegations. This conduct should even be applied if you leave Perrott Hill and are no longer a member of staff. With information often passed through 'friends of friends', by including pupils or even ex pupils you could inadvertently compromise the privacy of others.

It is best practice that staff should not include parents within their 'social networking' as this may lead to compromising the staff/parent professional relationship.

Another danger for teachers is posting compromising pictures of themselves on sites that could then be accessed by the public and/or the media. It is imperative that staff maintain professional standards and avoid bringing their profession and the School into disrepute. Employees are directed to the points of advice listed below with regards to settings.

There are recorded incidents of pupils setting up 'imposter' social networking accounts and this has not been helped with the widespread use of mobile phones with cameras (which enables embarrassing pictures to be taken and easily posted). If this occurs, then the Head and ICT Systems and Development Manager are to be informed.

If staff wish to access social networking sites whilst at work, then this must only be done as part of a reasonable 'break' and on their own personal computer or mobile device (when not directly in charge of pupils) or only on one of the three workstations in the staffroom. 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.

Where staff are using social networking, it is important to:
- observe this Staff Acceptable Use Policy and other School policies, particularly the 'Staff Code of Conduct' and any others with respect to confidentiality, safeguarding, professional boundaries and data protection; - 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'. It is now possible to

approve any photo or post before it becomes visible to anyone via your profile; however, this option must be activated.

- Avoid adding students or past students and it is best practice not to add parents to your list of contacts (see above).
- Take very great care in adding ex-colleagues as 'friends' as they may have friends – or become so in the future – who are current or past pupils or parents. This is a distinct possibility with Gap students in particular. Settings must be very carefully managed to ensure the mutual 'friend' does not act as a bridge that allows those pupils/parents to access your profile.
- Maintain professional standards at all times.
- Never write/post or upload images that could be interpreted as unprofessional.
- Avoid posting information about the School, pupils, past pupils, pupils' families or members of staff (past or present), including photographs.
- Clearly request that your friends do not post information or photographs that could be interpreted as incriminating.
- If you have (by accident) "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

Where ever possible, staff may not use their personal devices while they are directly in charge of pupils or whilst carrying out their role at Perrott Hill School, other than in case of emergency such as a lockdown procedure or extremely urgent School business when it must be safe to phone.

Personal devices should not be used to photograph, film or record (sound and visual) pupils by members of staff or whilst in the capacity of a volunteer.

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*.
- Digital images of children must be stored on the password protected area of the School's network.
- 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 and 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, please change your password immediately and inform the ICT Department of this concern. 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.

SECTION FOURTEEN

RESIDENT STAFF

Most of the School's residential accommodation has a computer outlet that connects to the School network. If a resident member of staff has an outlet within their accommodation, the School can provide them with their own Wi-Fi point setup for a personal 'home' network that can provide them internet access using the School's high speed fibre optic connection. The School's filtering system can also be setup so that any connection from this point will be unfiltered, no sites will be blocked and traffic and internet sites visited will not be logged on the School's filtering system. This would provide a connection similar to if those staff lived off-site. If resident staff require a personal 'home' network, a residential access request form can be obtained from the ICT Department.

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 (to be signed and a copy placed on staff file)

EMPLOYEE AGREEMENT ON USE OF 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 computers, networks, internet and telecommunications equipment and services. I understand that this includes the use of my personal technologies, for example my mobile phone or laptop etc. 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 of these guidelines on appropriate use of the e-mail and internet systems 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 the e-mail and internet 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.