HURLINGHAM SCHOOL

Policy regarding Acceptable Use of Computing and Online Safety, including Mobile Phones.

This policy is made available to all parents, prospective parents, staff and prospective employees of Hurlingham School on our website, and a hard copy can also be viewed at our School Office and applies to all aspects of Hurlingham School's work, including the Nursery and Early Years Foundation Stage (EYFS).

1) Scope of this Policy

This policy applies to all members of the school community, including staff, pupils, parents, carers, and visitors. In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers (but access to systems is not intended in any way to imply an employment relationship). 'Parents' include, where applicable, pupils' carers and those with parental responsibility. 'Visitors' includes anyone else who comes to the school, including occasional volunteers.

2) Other Related Policies

This policy has clear links to other policies in our school, in particular to:

- Anti-Bullying Policy
- Behaviour, Rewards, Sanctions, Discipline and Exclusions Policy
- Health and Safety Policies
- Safeguarding and Safer Recruitment Policy (including PREVENT guidance)
- Safeguarding and Child Protection Policy
- Computing Policy
- PSHEE Policy
- Data Protection Policy
- Taking, Using and Storing Images of Children Policy
- e-Safety Policy
- Bring your Own Device (BYOD) Policy for Staff and Visitors (Appendix 1)
- Privacy Notice (for pupils, parents, carers and staff)
- Staff Code of Conduct.
- Staff Record Keeping Policy
- Data Retention Policy and Retention Guidelines
- Whistleblowing Policy
- Data Breach Reporting Policy

Each of these policies is concerned with the protection of all children in the school from various kinds of harm and they all contained within our Staff Handbook.

3) Online behaviour

As a member of the school community you should follow these principles in all of your online activities:

- Ensure that your online communications, and any content you share online, are respectful of others and composed in a way you would wish to stand by.
- Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the school or wider community (for example, content that is obscene, or promotes violence, discrimination, or extremism, or raises safeguarding issues).
- Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the school community, even if the content is not shared publicly, without going through official channels and obtaining permission.
- Do not access or share material that infringes copyright, and do not claim the work of others as your own.
- Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.
- Staff should not use their personal email, or social media accounts to contact pupils or parents, and pupils and parents should not attempt to discover or contact the personal email addresses or social media accounts of staff.

4) Using the School's IT systems

Users are encouraged to make use of the school computing facilities for educational purposes. All users are expected to act responsibly and to show consideration to others.

Whenever you use the school's IT systems (including by connecting your own device to the network) you should follow these principles:

- Only access school IT systems using your own username and password. Do not share your username or password with anyone else.
- Do not attempt to circumvent the content filters or other security measures installed on the school's IT systems, and do not attempt to access parts of the system that you do not have permission to access.
- Do not attempt to install software on, or otherwise alter, school IT systems.
- Do not use the school's IT systems in a way that breaches the principles of online behaviour set out above.

Remember that the school monitors use of the school's IT systems, and that the school can view content accessed or sent via its systems. It is not acceptable to:

- Attempt to download to, install or run software on a school owned computer unless previously agreed with the Head of Media and Computing Resources.
- Attempt to copy or remove software from a school computer unless previously agreed with the Head of Media and Computing Resources.
- Attempt to introduce a virus, or malicious code.
- Attempt to bypass network and systems security including content filters. All online content entering the building is filtered and may be monitored.
- Attempt to initiate remote access from outside the school network without permission from the Head of Media and Computing Resources.
- Attempt to access another user's account.
- Attempt to gain access to an unauthorised area or system either in person or electronically.
- Attempt to use any form of hacking or cracking software / system.
- Connect or install a Wireless Access Point directly to the network or via a computer. However, should

the internet connection be unavailable and an urgent replacement needed for office communication purposes, the Head of Media and Computing Resources, Headmaster or Principal may initiate a temporary wireless dongle link.

- Connect or install any device to access the internet not previously approved by the Head of Media and Computing Resources such as modem, broadband or internet enabled mobile phones directly to the network or via a computer.
- Access, download, create, store or transmit material which is indecent or obscene, or material which could cause annoyance, offence or anxiety to other users, or material which infringes copyright, or material which is unlawful.
- Engage in activities which waste technical support time and resources.

5) Passwords and Logging on Securely

- Passwords protect the School's network and computer system and are your responsibility. They should not be obvious (for example "password", 123456, a family name or birthdays), and nor should they be the same as your widely-used personal passwords (Google Apps email passwords should be judged as strong).
- Staff passwords have an expiry time of 365 days and must be changed when reminded at the start of each Autumn term.
- Student passwords do not expire and can only be changed by the Head of Media and Computing Resources.
- You should not let anyone else know your password, nor keep a list of passwords where they may be accessed, and must change it immediately if it appears to be compromised.
- You should not attempt to gain unauthorised access to anyone else's computer or to confidential information to which you do not have access rights. Users must not log on as someone else, nor use a computer which has been logged on by someone else.
- Users must log off when leaving a workstation, even for a short time, or lock the workstation if no other user is likely to need to use it.

6) Use of Property

Any property belonging to the School should be treated with respect and care, and used only in accordance with any training and policies provided. You must report any faults or breakages without delay to Head of Media and Computing Resources.

7) Use of School Systems

The provision of school email accounts, Wi-Fi and internet access is for official school business, administration and education. Staff and pupils should keep their personal, family and social lives separate from their school IT use and limit as far as possible any personal use of these accounts. Again, please be aware of the school's right to monitor and access web history and email use.

8) Use of personal devices or accounts and working remotely

All official school business must be conducted on school systems, and it is not permissible to use personal email accounts for school business. Any use of personal devices for school purposes, and any removal of personal data or confidential information from school systems – by any means including email, printing, file transfer, cloud or (encrypted) memory stick – must be registered and approved by the Headmaster or the Head of Media and Computing Resources.

Where permission is given for use of personal devices, these must be subject to appropriate safeguards in line with the school's policies, including two-factor authentication or encryption etc.

Use of portable storage devices

Including, but not limited to, USB memory sticks, portable hard drives, CDs, DVDs, mobile telephones, MP3

players and cameras.

- Pupils are not allowed to bring mobile telephones into school. The only exception to this is when a Year 6 child has begun to commute independently during their final term. Under such circumstances the phone must be handed to the class teacher at the start of the day and collected just before leaving the building in the afternoon. We recommend that children are supplied with very basic phones for this purpose. No child is, therefore, allowed to use their own mobile phone during the school day.
- Pupils may not bring portable storage devices into school.
- It is essential that members of staff ensure that, while working with pupils in EYFS, all mobile phones are not used and are put fully away into a bag or pocket. In the case of pupils of Reception age, this is a legal requirement. The only exception is in the event of an emergency in order to summon help. Staff must report anyone found using a mobile telephone in the presence of EYFS pupils to a member of the SLT immediately.
- The preferred means of transfer of data is through the school's email system. However, Google Drives may also be used for the transfer of larger files if necessary.
- All devices containing software which includes parents', pupils' or staff personal details should be encrypted at all times.
- It is the responsibility of members of staff to ensure that any storage device brought into school has only been connected to a computer which the staff member knows to have active and up to date antivirus software, and for that computer to be free of viruses and malicious software.
- It is the responsibility of members of staff to ensure that any storage device that they own does not contain private or confidential information about any individual or group of people. This extends to devices which may have been used to take photographs, videos and other electronic recordings. Such files should be removed from the devices at the earliest possible opportunity and stored securely on the school network.
- Portable storage devices must be manually scanned with the school's anti-virus software before any files are transferred or opened. If you are unsure of how to do this, please ask the Head of Media and Computing Resources.
- Once data is transferred the device should be disconnected from the computer.
- Data should only be temporarily stored on portable storage devices and in accordance with the school's data protection policy and should be encrypted.
- No social networking sites should ever be used as part of any employee's work or activities associated with the school in any way.
- No functions within mobile telephones should ever be used in a room where children are present unless a specific reason requires their application and this is explained to the pupils at the time.
- Children must never be photographed by cameras built into mobile phones, the only exception may be for the use of school owned property which should then be returned to the Head of Computer and Media Resources or occasions in which the Headmaster or Principal (but no one acting in their stead) has given explicit permission. Any image taken under such circumstances must be transferred to the school network at the earliest opportunity and then deleted from the phone and any auto backup service.
- Should a photograph of a child be taken using a digital camera, the image must be transferred onto the school network media drives at the first possible opportunity and the file on the camera must then be deleted. No images of children should ever be uploaded to photo or video sharing sites.
- On no account must mobile telephones be used in the presence of one or more EYFS children unless an emergency call is being made.

9) Monitoring and Managing Access and Security

Staff, parents and pupils should be aware that school email and internet usage (including through school Wi-Fi) will be monitored for safeguarding, conduct and performance purposes, and both web history and school email

accounts may be accessed by the school where necessary for a lawful purpose – including serious conduct or welfare concerns, extremism and the protection of others.

Any personal devices used by pupils, whether or not such use is permitted, may be confiscated and examined under such circumstances. The school may require staff to conduct searches of their personal accounts or devices if they were used for school business in contravention of this policy.

The school will provide managed internet access to its staff and pupils in order to help pupils to learn how to assess and manage risk, to gain the knowledge and understanding to keep themselves safe when using the internet and to bridge the gap between school IT systems and the more open systems outside school.

- The school will use a recognised internet service, currently Vaioni.
- The school will ensure that all internet access has age appropriate filtering provided by a recognised filtering system which is regularly checked to ensure that it is working, effective and reasonable, currently through OpenDNS.
- The school will ensure that its networks have virus and anti-spam protection, currently ESET Endpoint.
- Access to school networks will be controlled by personal passwords.
- Systems will be in place to ensure that internet use can be monitored and a log of any incidents will be kept to help to identify patterns of behaviour and to inform e-safety policy.
- The security of school ICT systems will be reviewed regularly by the Head of Media and Computing Resources in conjunction with the Principal.
- The school will ensure that access to the internet via school equipment for anyone not employed by the school is similarly filtered and monitored.

10) Compliance with related school policies

All staff, pupils, parents and adults engaged in work for and on behalf of Hurlingham School must comply with the school's e-Safety Policy and all of the other Policies and documents listed in the 'other related policies' above.

11) Retention of digital data

Teaching staff must be aware that all emails sent or received on school systems will be routinely deleted after 4 years and email accounts will be closed and the contents within 6 months of that person leaving the school. Important information that is necessary to be kept should be held on the relevant personnel or pupil file, not kept in personal folders, archives or inboxes. Hence it is the responsibility of each account user to ensure that important information (or indeed any personal information that they wish to keep, in line with school policy on personal use) is retained in the right place or, where applicable, provided to the right colleague. That way no important information should ever be lost as a result of the school's email deletion protocol.

If you consider that reasons exist for the protocol not to apply, or need assistance in how to retain and appropriately archive data, please contact The Head of Media and Computing Resources.

12) Roles and Responsibilities

Teachers will:

- ensure all children know and understand the relevant page(s) in their Homework Diary or other homelink book regarding Safe and Sensible Computing. Once satisfactory knowledge and understanding have been achieved by children, teachers will ensure the relevant page is signed by both the child and their parents;
- deliver planned provision for sensible computer use and safe conduct on the Internet as detailed in the Schemes of Work for PSHEE (and Computing);
- inform the Head of PSHEE of any amendments to topics or themes, thereby ensuring the monitoring of continuity and breadth in our educational provision concerning online safety and sensible computer use.

The Headteacher, in conjunction with the Head of PSHEE, will:

- monitor delivery of the syllabus to ensure children understand the importance of staying safe and acting sensibly when using computers and surfing the Internet;
- ensure that clear guidance regarding online safety and sensible computing is disseminated to all parents on at least an annual basis through Welcome Evenings at the start of the academic year (which, for older children, are arranged back-to-back in every other year with a briefing on internet safety from an external provider,) followed up by a statement in each child's Homework Diary, signed by the pupil and at least one parent;
- lead the development of online safety in the curriculum and resources;
- teach demonstration lessons if appropriate;
- provide support and guidance to all staff;
- prepare and lead INSET on E-Safety, as appropriate. The Headmaster is a trained and qualified CEOP Ambassador; he takes staff members through the key CEOP training messages on a regular basis.
- attend relevant courses/meetings and disseminate information to colleagues;
- monitor incidents of e-safety concern throughout the term and report concerns to staff and the Principal (DMS) whenever appropriate. The Principal will include any online safety or sensible computing concerns in her annual report on Child Protection and Safeguarding to the Boards of Advisors and Directors.
- review the impact of policy and procedures against the number of incidents.

13) Use of the network and computer facilities

Use of the Internet

Access to the Internet is filtered to prevent access to inappropriate sites, and to protect the computer systems. Users should be aware that the school logs all Internet use for students and for staff.

- The use of public chat rooms or messaging services (such as MSN, AOL or ICQ) is not allowed, other than Hurlingham School email chat.
- Users should not copy and use material from the Internet to gain unfair advantage in their studies, for example in course work. Such actions may lead to disqualification by examination boards.
- Users should ensure that they are not breaking copyright restrictions when copying and using material from the Internet.
- The use of the Internet during all school activities is under the direction of the teacher.

Use of email

Automated software scans all e-mail, and removes anything which could affect the security of the computer systems.

- Pupils are not allowed to use email or chat software during lessons, unless the teacher for that lesson has allowed its use.
- If a user receives an e-mail which is offensive or upsetting, the headmaster (or in the case of a pupil, the form teacher who will pass the information on to the Headmaster) should be contacted immediately. Do not delete the email in question until the matter has been investigated.
- If the sender of the offensive email is the headmaster, the School Principal should be contacted.
- SPAM email received should be reported by pressing the 'Report Spam' button.
- The sending / forwarding of chain e-mails are not permitted.
- The sending of bulk e-mails is acceptable only for good reason associated with school. Before doing so, the user must obtain permission from the Head of Media and Computing Resources.
- All externally addressed group emails should be addressed in the TO: field to office@hurlinghamschool.co.uk (or left blank) and the individual recipients' email addresses entered in the BCC: field

- Do not open attachments from senders you do not recognize, or that look suspicious.
- Users of school computers and users involved in school business, may only use the e-mail accounts set up by the School.

Printing and Copying
All printing and photocopying within the school is logged by printer and by user.

Personal Laptops and Computers
Personal laptops and computers are not allowed to be connected to the school network or brought into school without permission from the Head of Media and Computing Resources and the Headmaster.
The school has a set of laptops, which staff may arrange to borrow with approval from the Head of Media and Computing Resources.

14) Privacy and Personal Protection

('Users' are all staff, pupils, parents and adults engaged in work for and on behalf of Hurlingham School)

- Users must at all times respect the privacy of other users.
- Users should not supply personal information about themselves or others, on websites, within email or instant messaging without permission from the headmaster.
- Users must not attempt to arrange meetings with anyone met via a website, email or instant messaging.
- No member of staff should be a 'friend' on any social network with a current pupil or past pupil under the age of 18. It may also be considered inappropriate above this age.
- Staff must not upload images of children to the Internet at any time without explicit permission from the Headmaster on each occasion.
- Staff must not upload any image of colleagues, named or not, without their permission.
- All staff should be aware that the images that they upload of themselves to the Internet should not bring themselves or the school into disrepute (e.g. extra care should be taken if members of staff are 'friends' with school parents on social networks.) Should this be the case, disciplinary procedures may be initiated.
- Users should realise that the school has a right to access personal folders on the Network.
- Privacy will be respected unless there is reason to think that someone is not following the ICT Acceptable Use Policy or school guidelines.

15) Disciplinary Procedures

Those who misuse the computer facilities and break the ICT Acceptable Use Policy will be subject to disciplinary procedures as outlined in their contract or staff handbook.

16) ICT Support

If you have any questions, comments or requests with regards to the ICT Systems in place, do not hesitate to contact the Head of Media and Computing Resources.

Faulty equipment should be reported to the Head of Media and Computing Resources, by email or in person, who will deal with issues on the basis of their specific urgency and how it impacts upon teaching and learning. Users should not attempt to repair equipment themselves.

17) Breach reporting

The law requires the school to notify personal data breaches, if they are likely to cause harm, to the authorities and, in some cases, to those affected. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This will include almost any loss of, or compromise to, personal data held by the school regardless of whether the personal data falls into a third party's hands. This would include:

- loss of an unencrypted laptop, USB stick or a physical file containing personal data;
- any external hacking of the school's systems, eg through the use of malware;
- application of the wrong privacy settings to online systems;
- misdirected post, fax or email;
- failing to bcc recipients of a mass email; and
- unsecure disposal.

The school must generally report personal data breaches to the ICO without undue delay (ie within 72 hours), and certainly if it presents a risk to individuals. In addition, controllers must notify individuals affected if that risk is high. In any event, the school must keep a record of any personal data breaches, regardless of whether we need to notify the ICO.

If either staff or pupils become aware of a suspected breach they should contact the Principal in the case of staff and children should notify their teacher.

Data breaches will happen to all organisations, but the school must take steps to ensure they are as rare and limited as possible and that, when they do happen, the worst effects are contained and mitigated. This requires the involvement and support of all staff and pupils. The School's primary interest and responsibility is in protecting potential victims and having visibility of how effective its policies and training are. Accordingly, falling victim to a data breach, either by human error or malicious attack, will not always be the result of a serious conduct issue or breach of policy; but failure to report a breach will be a disciplinary offence.

18) Breaches of this policy

A deliberate breach of this policy will be dealt with as a disciplinary matter using the School's usual procedures. In addition, a deliberate breach may result in the school restricting your access to school IT systems.

If you become aware of a breach of this policy or the e-Safety Policy, or you are concerned that a member of the school community is being harassed or harmed online you should report it to the Headmaster or Principal who is also the Designated Member of Staff for Safeguarding and the School's Data controller. Reports will be treated in confidence.

19) Acceptance of this policy

Please confirm that you understand and accept this policy by signing below and returning the signed copy to the School Office.

I understand and accept this acceptable use policy (staff):

Name: ……

Signature: ……

Date: ……

For younger pupils (below secondary school age)

Name of parent/guardian: ……

Signature: ……

Date: ……

Date created: Autumn 2010
Date of last review: June 2018
Date of next review: June 2019