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) Introduction

It our duty to ensure that every pupil in our care is safe; and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking, abuse and radicalisation.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used in and outside of school include:

- Websites;
- Email and instant messaging;
- Blogs;
- Social networking sites;
- Chat rooms;
- Music / video downloads;
- Gaming sites;
- Text messaging and picture messaging;
- Video calls;
- Podcasting;
- Online communities via games consoles; and
- Mobile internet devices such as smart phones and tablets.

This policy, supported by the Policy Regarding Acceptable Use of Computing and Online Safety, including Mobile Phones Policy for all staff, visitors and pupils, is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policies:

- Safeguarding and Child Protection Policy
- Staff Code of Conduct;
- Health and Safety Policy;
- Behaviour, Rewards, Sanctions, Discipline and Exclusions Policy;
- Anti-Bullying Policy;
- Policy Regarding Acceptable Use of Computing and Online Safety, including Mobile Phones;
- Data Protection Policy;

- Bring Your Own Device (BYOD) Policy for Staff and Visitors; and
- PSHEE and Citizenship Policy.

Whilst exciting and beneficial both in and out of the context of education, much IT, particularly online resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

At Hurlingham, we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving pupils in discussions about e-safety and listening to their fears and anxieties as well as their thoughts and ideas.

2) Scope of this Policy

This policy applies to all members of the school community, including staff, pupils, parents and visitors, who have access to and are users of the school IT systems. In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers. 'Parents includes pupils' carers and guardians. 'Visitors' includes anyone else who comes to the school, including occasional volunteers.

Both this policy and the Acceptable Use Policy (for all staff, visitors and pupils) cover both fixed and mobile internet devices provided by the school (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.); as well as all devices owned by pupils, staff, or visitors and brought onto school premises (personal laptops, tablets, smart phones, etc.).

3) Roles and responsibilities

The Board of Directors

The Board of Directors of the school is responsible for the approval of this policy and for reviewing its effectiveness. The governing body will review this policy at least annually. The Principal is responsible for keeping the Board of Directors fully informed about the School's procedures in relation to e-safety.

The Headmaster and the Senior Leadership Team

The Headmaster is responsible for the safety of the members of the school community and this includes responsibility for e-safety.

In particular, the role of the Headmaster and the Senior Leadership team is to ensure that:

- staff, in particular the Head of Media and Computing Resources are adequately trained about e-safety; and
- staff are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of e-safety in connection to the school.

IT staff

The school's Head of Media and Computing Resources has a key role in maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments. He is responsible for the security of the school's hardware system, its data and for training the school's teaching and administrative staff in the use of IT. He monitors the use of the internet and emails, maintains content filters, and will report inappropriate usage to the Headmaster.

Teaching and support staff

All staff are required to sign the Policy Regarding Acceptable Use of Computing and Online Safety, including Mobile Phones before accessing the school's systems.

As with all issues of safety at this school, staff are encouraged to create a talking and listening culture in order to address any e-safety issues which may arise in classrooms on a daily basis.

Pupils

All pupils, from Year I upwards are required to sign and Accdptable Use agreement and Code of Conduct before accessing the School's systems. Pupils are responsible for using the school IT systems in accordance with the Acceptable Use Policy, and for letting staff know if they see IT systems being misused.

Parents and carers

Hurlingham School believes that it is essential for parents to be fully involved with promoting e-safety both in and outside of school. We regularly consult and discuss e-safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage. The school will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

Parents and carers are responsible for endorsing the school's Pupil Acceptable Use Policy.

4) Education and training

Staff: awareness and training

New staff receive information on our Policy Regarding Acceptable Use of Computing and Online Safety, including Mobile Phones as part of their induction.

All teaching staff receive regular information and training on e-safety issues in the form of INSET training and internal meeting time, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of e-safety.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. These behaviours are summarised in the Acceptable Use Policy which must be signed and returned before use of technologies in school. When children use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's IT guidelines.

Teaching staff are encouraged to incorporate e-safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community.

A record of concern must be completed by staff as soon as possible if any incident relating to e-safety occurs and be provided directly to the school's Headmaster.

Pupils: e-Safety in the curriculum

IT and online resources are used increasingly across the curriculum. We believe it is essential for e-safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote e-safety and regularly monitor and assess our pupils' understanding of it.

The school provides opportunities to teach about e-safety within a range of curriculum areas and IT lessons. Educating pupils on the dangers of technologies that may be encountered outside school will also be carried out via PSHEE, by presentations in assemblies, as well as informally when opportunities arise.

At age-appropriate levels, and usually via PSHEE, pupils are taught about their e-safety responsibilities and to look after their own online safety. From year 5, pupils are formally taught about recognising online sexual exploitation, stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across. Pupils can report concerns to the Headmaster and any member of staff at the school.

From year 6, pupils are also taught about relevant laws applicable to using the internet; such as data protection and intellectual property. Pupils are taught about respecting other people's information and images (etc.) through discussion and classroom activities.

Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Anti-bullying Policy, which describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying). Pupils should approach Headmaster, Head of Section or Principal as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

Parents

The school seeks to work closely with parents and guardians in promoting a culture of e-safety. The school will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

The school recognises that not all parents and guardians may feel equipped to protect their [son or daughter] when they use electronic equipment at home. The school therefore arranges biannual discussion evenings for parents when an outside specialist advises about e-safety and the practical steps that parents can take to minimise the potential dangers to their sons and daughters without curbing their natural enthusiasm and curiosity.

5) Policy Statements

Use of school and personal devices

Staff

School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. Staff should only use the school device which is allocated to them for school work. When they are not using a device staff should ensure that it is locked to prevent unauthorised access. Devices issued to staff are encrypted, to protect data stored on them.

Staff are referred to the Bring Your Own Device (BYOD) Policy for Staff and Visitors for further guidance on the use of non-school owned electronic devices for work purposes.

Personal telephone numbers, email addresses, or other contact details may not be shared with pupils or parents / carers and under no circumstances may staff contact a pupil or parent / carer using a personal telephone number, email address, social media, or other messaging system.

Pupils

Pupils in the Summer term of Form VI who commute to School independently should bring a mobile phone with them. These must be handed in to the Form teacher at the start of the day and collected from Reception as they leave school. Pupils are not allowed to bring in any other devices that communicate over the internet including smartwatches and other wearable technology.

School mobile technologies available for pupil use including laptops, tablets, cameras, etc. are stored in the IT office. Access is available via Head of Media and Computing Resources.

The school recognises that mobile devices are sometimes used by pupils for medical purposes or as an adjustment to assist pupils who have disabilities or special educational needs. Where a pupil needs to use a mobile device for such purposes, the pupil's parents or carers should arrange a meeting with the pupil’s Head of Section to agree how the school can appropriately support such use. The Head of Section will then inform the pupil's teachers and other relevant members of staff about how the pupil will use the device at school.

Use of internet and email

Staff

Staff must not access any website or personal email which is unconnected with school work or business from school devices or whilst teaching. Such access may only be made from staff members' own devices whilst away from the presence of pupils.

When accessed from staff members' own devices / off school premises, staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the school.

The school has taken all reasonable steps to ensure that the school network is safe and secure. Staff should be aware that email communications through the school network and staff email addresses are monitored.

Staff must immediately report to the Headmaster or in his absence the Deputy Head the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to the Head of Media and Computing Resources.

Any online communications must not either knowingly or recklessly:

- place a child or young person at risk of harm, or cause actual harm;
- bring Hurlingham into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
    - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
    - using social media to bully another individual; or
    - posting links to or endorsing material which is discriminatory or offensive.

Under no circumstances should school pupils, parents or former pupils under the age of 18 be added as social network 'friends' or contacted through social media.

Any digital communication between staff and pupils or parents / carers must be professional in tone and content. Under no circumstances may staff contact a pupil or parent / carer using any personal email address. The school ensures that staff have access to their work email address when offsite, for use as necessary on school business.

Pupils

There is strong anti-virus and firewall protection on our network.

Pupils must not respond to any website or other communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication, to their class teacher, computing teacher or any other member of staff.

The school expects pupils to think carefully before they post any information online, or repost or endorse content created by other people. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others.

Pupils must report any accidental access to materials of an inappropriate nature directly to their class teacher, computing teacher or any other member of staff. Deliberate access to any inappropriate materials by a pupil will lead to the incident being reported to the Headmaster and will be dealt with under the school's Behaviour, Rewards, Sanctions and Exclusion Policy. Pupils should be aware that all internet usage via the school's systems and its wifi network is monitored.

Certain websites are automatically blocked by the school's filtering system. If this causes problems for school work / research purposes, pupils should contact the Head of Media and Computing for assistance.

6) Data storage and processing

The school takes its compliance with the Data Protection Act 1998 seriously. Please refer to the Data Protection Policy and the Policy Regarding Acceptable Use of Computing and Online Safety, including Mobile Phones; for further details.

Staff and pupils are expected to save all data relating to their work to either the staff drive or to the Pupils' drive on the school's central server.

Staff devices should be coded if any data or passwords are stored on them. The school expects all removable media (USB memory sticks, CDs, portable drives) taken outside school or sent by post or courier to be coded before sending.

Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or pupils should be stored on personal memory sticks, but instead stored on an encrypted USB memory stick provided by school or Google drive.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the Headmaster.

7) Password security

Staff have individual school network logins, email addresses and storage folders on the server. Staff are regularly reminded of the need for password security.

All staff members of staff should:

- use a strong password (usually containing eight characters or more, and containing upper and lower case letters as well as numbers), which should be changed every [6] months;
- not write passwords down; and
- not share passwords with other pupils or staff.

8) Safe use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet.

Parents / carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published on blogs or social networking sites (etc.) without the permission of the parents of children identifiable in them (or in the case of adults the permission of the individuals themselves). The most senior members of staff present at any play or performance reminds parents of this requirement.

Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow this policy and the Policy Regarding Acceptable Use of Computing and Online Safety, including Mobile Phones concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment: personal equipment should not be used for such purposes.

Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Written permission from parents or carers will be obtained before photographs of pupils are published on the school website (see Parent Contract / Acceptable Use Policy for more information).

Photographs published on the school website, or displayed elsewhere, that include pupils, will be selected carefully and will comply with good practice guidance on the use of such images. Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

9) Misuse

Hurlingham School will not tolerate illegal activities or activities that are inappropriate in a school context, and will report illegal activity to the police and/or the LSCB. If the school discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the CEOP

Incidents of misuse or suspected misuse must be dealt with by staff in accordance with [the school's policies and procedures (in particular the Safeguarding Policy).

The school will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our Anti-Bullying Policy.

10) Complaints

As with all issues of safety at Hurlingham School, if a member of staff, a pupil or a parent / carer has a complaint or concern relating to e-safety prompt action will be taken to deal with it. Complaints should be addressed to the appropriate Head of section who will undertake an investigation where appropriate. Please see the Complaints Policy for further information.

Incidents of or concerns around e-safety will be recorded using a Record of Concern form and reported to the school's Headmaster and/or the Designated Safeguarding Lead, in accordance with the school's Child Protection Policy.

Date Created: January 2017
Date of Last Review: May 2018
Date of Next Review: May 2019