Hampton Junior School

Online Safety Policy

Version	Date	Comments
1	2018	

Online Safety Policy

Introduction

Technology is developing at an increasing rate and, year on year, impacts the lives of citizens and education. While developing technology brings many opportunities, it also brings risks and potential dangers. Through our Online Safety Policy we aim to reduce the risk to our students by:

- Protecting and educating pupils and staff in their use of technology.
- Outlining appropriate mechanisms to intervene and support any online safety incidents at home or in school.
- Providing clear advice and guidance on how to minimise risks and how to deal with any infringements of school policy.

The policy applies to all members of the school community both within and outside of school. The purpose of this policy is to ensure that all staff, parents, governors and children understand and agree the school's approach to online safety. This policy relates to other policies including Behaviour, Safeguarding, Health and Safety and Facebook.

Responsibilities

At HJS we believe that all staff and children have a **shared responsibility for online safety** and that ICT usage by all network users is safe and secure. The Headteacher, with the support of the Governing Body, aims to embed safe practices into the culture of the school. The Headteacher ensures that the policy is implemented and compliance with the policy is monitored.

Our Designated Safeguarding Lead, Jon James, and our Deputy Designated Safeguarding Lead, Helen Lockey, ensures they keep up to date with online safety issues and guidance through organisations such as LGfL & Child Exploitation and Online Protection (CEOP). The Designated Safeguarding Lead ensures the Headteacher, senior leadership, staff and Governors are updated as necessary.

Governors have an overview understanding of online safety issues and strategies at HJS. The Designated Safeguarding Lead will update the Governing Body at least once a year to ensure that governors are aware of changes in local and national guidance.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms. All staff are required to sign the school's Acceptable Use Agreement (see Appendix A). The signed copies are kept in the individual member of staff's file and a copy is available in the staffroom to refer to if necessary. Staff are reminded / updated about online safety issues at least once a year.

Children's Rules for using technology at school.

These are the rules that have been developed with our governors, staff, parents and children:

1. Keep passwords safe.
2. Keep communication polite.
3. Keep your personal information safe from strangers.
4. Keep your parents and responsible adults in school informed of anything that upsets you when using technology.
5. Keep away from sites that you are not permitted to access.

The school takes all reasonable precautions to prevent access to inappropriate material. We have a managed system which we feel enables our children to understand how to deal with online safety incidents. This system is managed through Richmond Borough. As such, the school internet feed is filtered through LGfL (London Grid for Learning). However, due to the international scale and linked

nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience. This is particularly important for helping children to stay safe out of school where technical support and filtering may not be available to them.

All users have a responsibility to report immediately to class teachers / the Headteacher any infringements of the school's filtering system of which they become aware or any sites that are accessed, which they believe should be blocked.

Pupils are made aware of the importance of filtering systems through the school's Online Safety Curriculum. They will read and sign the Acceptable Use Agreement, which will be included in their Year 3 Welcome Pack (see appendix B).

Staff users will be made aware of the filtering systems through the Acceptable Use Agreement (as part of their induction process) and through briefing in staff meetings, training days, memos etc

Parents play an essential role in the education of their children and in the monitoring and regulation of the children's online experiences. The school will therefore seek to provide information and awareness to parents and carers through the Acceptable Use Agreement, letters, newsletters, web site and parents' evenings etc

Teaching and Learning

The purpose of Internet access in school is to raise educational standards, to support the professional work of staff and to enhance the school's management information and business administration systems. Access to the Internet is a necessary tool for staff and students. It helps to prepare students for their on-going career and personal development needs. Internet use enhances learning and is planned to enrich and extend learning activities. Staff select sites which support the learning outcomes planned for pupils' age and maturity.

As part of the Computing National Curriculum, pupils should be taught to "use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour and identify a range of ways to report concerns about content and contact." Therefore, we have a planned and progressive curriculum that also incorporates the Ofsted 'Keeping Children Safe in Education' guidelines September 2016.

Online Safety education will be provided in the following ways:

- A planned Online Safety programme will be provided as part of Computing, PHSE and other lessons and will be regularly revisited. This will cover both the use of ICT and new technologies in school and outside school.
- Key online safety messages should be reinforced through further input via assemblies (Safer Internet Day) and pastoral activities as well as informal conversations when the opportunity arises.
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use of ICT both within and outside school.
- Pupils should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information they find.

Managing Internet Access

The school ICT system security is reviewed regularly. Virus protection is updated regularly. Security strategies are discussed with the Local Authority.

Pupils are allowed to use school email accounts only. Pupils must tell a teacher immediately if they receive offensive email. In emails, pupils are taught that they must not reveal their personal details, those of others or arrange to meet anyone without specific permission. Pupils are taught not to open suspicious incoming email or attachments. The forwarding of chain letters is not permitted.

Passwords

Staff and pupils should always keep their passwords private, must not share with others and if a password is compromised the school should be notified immediately. All staff have their own unique username and private passwords to access school systems. We require staff to use strong passwords and to change their passwords twice annually when prompted to do so. Staff using critical systems are required to use two factor authentication.

E-mail

E-mail is now an essential means of communication for staff at HJS. We:

- Use the LGfL email on the school system for professional purposes.
- Do not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, for any communication with the wider public.
- Contact the police if one of our staff receives an e-mail that we consider is particularly disturbing or breaks the law.
- Manage accounts effectively, with up to date account details of users.
- May block access in school to external personal email accounts.
- Do not use email to transfer staff or pupil personal data unless anonymised.
- Teach pupils about the online safety of using e-mail both in school and at home.

The school website

The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained. The school web site complies with statutory DFE requirements. Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status. Children's photographs are only allowed to go on the website if written permission is held from the child's parents. The contact details on the website are for school admin only.

Social networking and personal publishing

Reference should not be made in social media to students/pupils, parents/carers or school staff. School staff should not be online friends with any current or former pupil/student nor should they engage in online discussion on personal matters relating to members of the school community.

Personal opinions should not be attributed to the school or local authority and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute.

Pupils will not be allowed to access public chat rooms. New applications are thoroughly tested before pupils are given access. Pupils are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our Online Safety Curriculum. Students are required to sign and follow our pupil Acceptable Use Agreement.

The Headteacher ensures that occasional checks are made to certify that the filtering methods selected are effective in practice. If staff or pupils discover unsuitable sites, the URL (address) and

content must be reported to the Internet Service Provider via the Headteacher or the Computing Lead.

Parents are reminded about social networking risks and protocols through our parental Acceptable Use Agreement. Parents are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.

Mobile Devices

Currently, our policy is that members of staff are permitted to bring their personal mobile devices into school. They are required to use their own professional judgement as to when it is appropriate to use them. Pupils are not currently permitted to bring their personal hand held devices into lessons. Years 5 & 6 are allowed to book their phones in at the school office each day (named and switched off). If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office. Mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile devices.

The recording, taking and sharing of images, video and audio on any personal mobile device is to be avoided. If a personal mobile device is used for such matters, the image or recording needs to be downloaded and fully removed from the mobile device the same day. The School reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying.

The sending of any abusive or inappropriate messages is forbidden. Consequences in accordance with our Behaviour Policy will be adhered to in such incidences.

Use of digital and video images

- When using digital images, staff should teach children to recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are allowed to take digital still and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images.
- Pupils must not take, use, share, publish or distribute images of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.
- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement when their daughter / son joins the school.
- Staff sign the school's Acceptable Use Agreement.
- The school blocks/filters access to social networking sites unless there is a specific approved educational purpose.
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Data Security

Staff must report any incidents where data protection may have been compromised to the Headteacher. We ensure staff know who to report such incidents to.

Staff have secure area(s) on the network to store sensitive files. We require staff to logout of systems when leaving their computer, but also enforce lock-out after 30 minutes idle time. All servers are managed by DBS-checked staff.

Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. Staff must not keep confidential information on removable devices such as USB devices unless suitably security protected.

Staff training

It is essential that all staff receive online safety training and understand their responsibilities, including ensuring that they fully understand the school's Online Safety Policy and Acceptable Use Agreements which are signed as part of their induction. The Designated Safeguarding Lead will also provide advice, guidance and training as required to individual. Governors should also take part in online safety training / awareness sessions.

Acceptable Use Agreement

All members of the school community are responsible for using the school ICT systems in accordance with the appropriate Acceptable Use Agreement, which they will be expected to sign before being given access to school systems.

Acceptable Use Agreements are revisited annually, and amended if necessary (requiring resigning), in light of new developments.

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to unsuitable content or which promote any kind of discrimination.

The school's Online Safety Policy and its implementation will be monitored and reviewed on a regular basis.

Complaints of internet misuse, including staff misuse, must be referred to the Headteacher. Complaints of a child protection nature must be dealt with in accordance with our Safeguarding Policy. Pupils and parents are informed of the complaints procedure. Pupils and parents are informed of the consequences for pupil misuse.

Failure to comply with our Acceptable Use Policy, either in or outside of school, will require the children involved and their parents to meet with the Headteacher, potentially receiving consequences in accordance with our Behaviour Policy.

Responding to online incidents and safeguarding concerns.

- The Designated Safeguarding Lead (DSL) will be informed of any online safety incidents involving child protection concerns, which will then be recorded.
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies.

- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.
- The school will manage online safety incidents in accordance with the school discipline/behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- Parents and children will need to work in partnership with the school to resolve issues.

Appendix A

Staff Acceptable Use of Information and Communications Technology Agreement

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct agreement.

- I have read and understood the Hampton Junior School Online Safety Policy.
- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the Designated Safeguarding Lead.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote online safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Information Systems Code of Conduct.

Signed: …… Capitals: …… Date: ……

Appendix B

Information and Communications Technology Acceptable use of Internet Agreement Pupil and Parent Agreement

When I use the Internet, social media and email, I will keep to these rules:

- I will only use the Internet with permission and only when there is a teacher or LSA present.
- I will not try to find unsuitable sites on the Internet and I will keep away from sites that I am not permitted to access.
- I will only email people I know or who my teacher has approved.
- The messages I send will be polite and sensible.
- I will not give my full name or home address or telephone number, or arrange to meet someone unless my parent, carer, or teacher has given permission.
- I will keep passwords safe.
- I will keep my parents and responsible adults in school informed of anything that upsets me when using technology.

Pupil's signature …….. Date: ……

Parent

As the parent or legal guardian of the pupil signing above, I give permission for my child to use electronic mail and the Internet, under supervision at school. I understand and accept the above rules for acceptable use of the Internet and will discuss these with my child.

Parents' signature …… Date ……

Pupil's name …… Class ……