HAMPTON SCHOOL TRUST

Online Safety Policy

Contents

1 Introduction

The policy applies to all schools within the Hampton School Trust ('the Trust' or 'the School') and to the members of the Trust's community who have access to and are users of Trust's IT systems, both in and out of the School. This includes:

a Pupils
b Staff – including teaching and support staff, contracted staff, governors and volunteers
c Parents – including carers and guardians
d Visitors – anybody else who enters the Trust's premises

This policy covers both fixed and mobile devices provided by the Trust, as well as devices owned by pupils, staff or visitors which are brought onto Trust premises. The policy, supported by the other relevant policies listed below, seeks to protect the safety of pupils and staff.

Whilst online communications and technology provide opportunities for enhances learning, they also pose great risks to young people and 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 bullying, harassment, grooming, abuse, stalking, identity theft and radicalisation. Improper use of mobile technology by pupils, in or out of School, will be dealt with under the relevant Behaviour policy.

2 Scope and Review

Technological developments such as the internet and other forms of electronic communication have great educational and social benefits, but they can also be used to harm others. Pupils are taught critical thinking skills enabling them to use technology to their advantage and teaching them appropriate behaviours when using the internet and related technologies in and beyond the classroom whilst also keeping them safe and operating within the law. Current and emerging technologies used in and outside of school include:

- Websites
- Email and instant messaging
- Blogs, forums and chat rooms
- Mobile internet devices (e.g. smart phones and tablets)
- Social networking sites
- Music/video downloads
- Gaming sites and communities formed via games consoles
- Instant messaging technology via SMs or social media sites
- Video calls
- Podcasting and mobile applications
- Virtual and augmented reality technology
- Artificial intelligence

The School is also committed to establishing a clear set of expectations regarding the online behaviour of both pupils and staff whilst also protecting the interests and safety of the School community.

3 Safety Responsibilities

All staff, governors and visitors have a responsibility to protect children from abuse of any sort and to make appropriate referrals. The following responsibilities should be read in conjunction with the School's **Safeguarding (Child Protection) Policy & Procedures**:

i. Hampton School

Online Safety is the responsibility of the Designated Safeguarding Lead (DSL), currently Owen Morris, Deputy Head (Pastoral)) and one of the Deputy Designated Safeguarding Leads (DDSL) Polly Holmes, Assistant Head (Pastoral). They work closely with the Head of PHSE, the Online Safety Officer, and with Pippa Message (Deputy Head) – a DDSL and Deputy Head with responsibility for IT at the Trust, and Mark Nicholson (Deputy Head) – a DDSL. The DSL and DDSLs work with the IT Department to ensure that the School's filtering and monitoring requirements are met and enforced and that regular checks are made.

The DSL is responsible for keeping up to date with current online safety issues and guidance issued by relevant organisations, including, but not restricted to, the Department for Education (including KCSiE), ISI and local Safeguarding partnerships.

ii. Hampton Pre-Prep & Prep

At Hampton Pre-Prep & Prep (HPP&P) Tammy Howard, the DSL and Deputy Head, has responsibility for online safety and works closely with the Head of Pre-Prep (Imogen Murphy), the DDSL.

iii. IT Department & ESafety Officer

The IT Department has a key role in maintaining a safe technical infrastructure. The Trust's network and email systems are filtered and monitored for inappropriate usage. Staff are given clear guidelines for the appropriate use of technology and detailed guidance is provided in the **Staff Behaviour Policy** which can be found on Cezanne in Documents area in the relevant Workspace.

The Online Safety Officer, along with the Deputy Heads and Head of Pre-Prep, will review the policy at least annually and amend as necessary.

iv. The Governing Body

The Governing Body has overall responsibility for safeguarding. It is also responsible for ratifying this policy and reviewing its effectiveness, at least annually.

The Governing Body, in conjunction with the Senior Leadership Teams (SLTs), will also ensure that all staff undergo safeguarding and child protection training at induction and thereafter at regular intervals to ensure that:

a. All staff, in particular the DSLs, DDSLs and the SLT, are adequately trained in Online Safety.
b. All staff are aware of the School's expectations with regard to Online Safety and how to raise concerns when identified.
c. All staff are aware of the School's policies and procedures that should be followed in the event of abuse or suspected breach of online safety in connection to the School.

v. Staff, Pupils & Parents

a. **Staff** – all staff are required to abide by the School's **IT Acceptable Use Policy** and by the **Staff Behaviour Policy** (and all other School policies). Staff are encouraged to address any safeguarding concerns or online safety issues either with the DSL/a DDSL or with a member of the SLT.
b. **Pupils** – all pupils are responsible for complying with the School's **Pupil IT Acceptable Use** policy and the **Pupil AI Acceptable Use** policy. They should also abide by the **Hampton Code of Conduct** or the **HPP&P School Code**.
c. **Parents**/Carers– The School strives to promote a wide understanding of the benefits and risks related to internet usage and will contact parents (including carers and guardians) should it have any concerns about a pupil's behaviour in relation to online safety. Likewise, parents are encouraged to share any concerns with the School.

4 Other Relevant Policies

This policy should be read in conjunction with the following Trust policies:

- Anti-Bullying Policy (which contains particular reference to Cyber-bullying and possible examples of this)
- Artificial Intelligence (AI)
- Behaviour, Rewards, Sanctions, Discipline and Exclusion*
- Hampton Code of Conduct
- Data Incident & Breach Policy
- Data Subject Rights Policy
- HPP&P School Code

- Pupil AI Acceptable Use
- Pupil IT Acceptable Use
- Safeguarding Policy
- Social Media Policy
- Staff Behaviour Policy
- Staff ICT Acceptable Use Policy
  *Denotes each school within the Trust has its own Behaviour policy

5 Education – Pupils

When joining Hampton School, all pupils are issued with their own personal school e-mail addresses for use on the School network and through remote access (whilst pupils at HPP&P are automatically given email addresses which allow functionality within School, they are told not to use them otherwise). This access is through a personal login which is password protected.

Staff and pupils are regularly reminded of the need for password security and it is emphasised that all members of the Trust should:

- Use a strong password
- Not write passwords down
- Not share passwords with others

Email communications are monitored and pupils are made aware of this.

Additionally, as part of the Admissions process, pupils are asked to read and sign a **Pupil IT Acceptable Use Agreement** which outlines protocols for the use of School equipment and their own devices. At HPP&P , this document is signed by pupils in Year 3 and upwards. Pupils in Years 1 and 2 are encouraged to discuss the Online Safety Agreement (KS1) at home with their parents. This Agreement goes to all children in Reception moving into Year 1, and then all new joiners in Year 1 and Year 2. Parents are asked to complete a form and all responses are tracked.

Pupils throughout the Trust are taught, at age-appropriate levels, about their online safety responsibilities and how to protect their own online safety. At Hampton, this is done during PHSE lessons and at HPP&P during Life Skills lessons.

Pupils are also taught that it is their duty to report any instances of exploitation, abuse, grooming (and similar) that they, or their peers, may be aware of. They are made aware of the relevant laws regarding the use of the internet, for example those that apply to data protection, online safety, respecting other people's information and images, and of the impact of cyber bullying. They are taught how to seek help if they are affected by any issue and this information is also displayed throughout the premises.

6 Education and Training – Staff

As part of their induction, staff receive information regarding online safety, including the School's expectations and applicable roles and responsibilities regarding filtering and monitoring. This policy will form part of the induction training. Further training takes place on INSET days, at the start of each term, and all staff are required to complete an annual online Safeguarding course.

Specific training is given to relevant staff for PSHE lessons, where more in-depth knowledge is required, and any relevant Safeguarding/Online Safety updates are communicated to all staff within the Trust.

In addition to the **Staff Behaviour Policy**, staff can also refer to the relevant **Common Room Handbook** for further advice with regard to use of the internet and staff communication with pupils. Teaching staff should ensure pupils are fully aware of the IT Acceptable Use Agreement when using School computers.

7 Education – Parents

Parents play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviour and the School seeks to work closely with parents to promote online safety

The School also arranges regular Year Group Pastoral Forums, and other events, where parents have the opportunity to discuss online safety and where advice is given as to how they can minimise the potential dangers to their children without curbing their enthusiasm. External speakers come into School on a regular basis to deliver an ESafety webinar.

At Hampton, parents receive communications via email giving advice on any matters that may arise and a termly Safeguarding letter, outlining any relevant national and local issues, is also sent. The School also distributes any guidance that may be published by the local authority.

At HPP&P regular updates are sent out in the School Bulletin with links to webinars, articles and podcasts. An annual workshop is also held for parents with external speakers (e.g. OpenView / Childnet) - all parents are invited to attend.

8 Use of devices, the internet, email and other forms of digital technology

The Trust sets out clear rules and guidance for pupils regarding the use of devices, digital technology and the Trust's network. Expectations are explained clearly in the Pupil **IT Acceptable Use Policy** which all pupils are required to sign and the **Staff IT Acceptable Use Policy** which staff sign as part of the recruitment process. Any School device assigned to a member of staff or to a pupil must have a password or device lock to prevent access by unauthorised person. Staff and Pupils must ensure devices are locked when not in use.

The School's expectations of pupils with regard to the use of devices are clearly set out in the **Hampton Code of Conduct** and **HPP&P School Code**. A device may be confiscated should it be found that a pupil has contravened the relevant Behaviour policy.

Expectations of staff use of the internet and other forms of digital technology, including photography, are set out in the **Staff Behaviour Policy.**

9 Filtering and Monitoring

The Trust has put in place appropriate filters and monitoring systems to protect children, while being mindful not to place unnecessary restrictions on their learning. The Trust uses Smoothwall to filter the content on the School network and also uses Smoothwall Monitor to monitor the online behaviour of users of the network (and use of School-issued laptops), to safeguard children from potentially harmful and inappropriate online material. The School fully complies with the Department for Education's published filtering and monitoring standards which set out that schools should:

- Identify and assign roles and responsibilities to manage filtering and monitoring systems.
- Review filtering and monitoring provision at least annually.
- Block harmful and inappropriate content without unreasonably impacting teaching and learning.
- Have effective monitoring strategies in place that meet their safeguarding needs.

In addition, the Trust has safeguarding screen-capture software that records and monitors key phrases and images to ensure content accessed via the School network is appropriate.

The filtering and monitoring software provides information and alerts on pupils' activity and behaviour on the School network and School laptops. Safeguarding staff (the DSL(s) and DDSLs , along with Mr R. Davieson (Online Safety Officer at Hampton School) review this information at least daily (on School working days) and any potential concerns are evaluated to ensure that they are addressed appropriately. Alerts received outside School hours or in School holidays may not be picked up until the next School term time working day.

The School's filtering and monitoring systems are designed to support child safeguarding, but parents remain primarily responsible for supervising their child's online activity outside School hours.

At Hampton School, the Online Safety Officer receives reports on pupil use of the School's network and online activity and the Deputy Heads receive reports on teaching and support staff use of the School's network and online activity. Should the need arise, the Safeguarding Team and Heads of Year are informed of any misuse. At HPP&P these protocols are carried out by the DSL and the DDSL. In addition, the Trust has safeguarding screen-capture software that records and monitors key phrases and images to ensure content accessed via the School network is appropriate.

Staff are reminded that should they have any concerns regarding the effectiveness of the filtering and monitoring system, they must report the matter to the DSL (or other member of the Safeguarding team) as soon as possible. Similarly, should they accidently access prohibited or inappropriate content, they should also report to the Safeguarding team.

If staff find that the system has inadvertently blocked access to websites that are used in school, they should report this to the IT Department via helpdesk@hamptonschool.org.uk.

Pupils are made aware that internet usage is monitored and they are advised that they must report any accidental access to unauthorised material to a member of the teaching staff. They should also report any websites that are normally used for school work should they be blocked.

10 Online Communications

i. **Staff**

Any digital communication between a member of staff and a pupil or parent(s)/carer(s) must be professional both in tone and content. Staff can refer to the Common Room Handbook for guidance. Staff have access to their School email address when offsite for use, as necessary, on School business. Personal contact details must not be shared with pupils, parents, carers or recent alumni (i.e. pupils over the age of 18 who have left the School within the last four years) or used to contact them. Neither should pupils, parents, carers or recent alumni be added to any social media network as 'friends'.

Should a member of staff receive any form of communication that makes them feel uncomfortable or that they feel is inappropriate, they should report this immediately to the DSL (or member of the Safeguarding team) and neither should they respond to any such communication. Should a member of staff feel that they are in receipt of a fraudulent email, they should report this immediately to the IT Department.

ii. **Pupils**

All pupils are given a School email address; pupils at HPP&P are told not to use it. Access is via a personal and password-protected login. Pupils should use this email for all School work and to make contact with members of staff; they should not use a personal email.

Pupils are taught to advise a member of staff immediately should they receive a communication which makes them feel uncomfortable in any way, and to not respond to any such communication.

Pupils are made aware that email communications through the School's network are monitored.

iii. **Alumni Relations (Development Office)**

Staff in the Development Office are permitted to contact recent alumni through online channels for the purpose of promoting alumni relations. These members of staff also receive appropriate training.

iv. **Trips & Activities**

Should there be any deviation from the Educational Trips policy with regard to communication between staff and pupils whilst on a trip, protocols will be agreed upon in advance and will be included in that trip's risk assessment.

11 Use of Social Media

Staff should familiarise themselves with the School's Social Media policy (H09) which clearly outlines expectations regarding the use of social media by all staff.

12 Safe Use of Digital Images

The School informs and educates pupils about the risks associated with the taking, use, sharing, publication and distribution of images.

Staff can refer to Appendix 4 of the School's Privacy Notice.

13 Artificial Intelligence

The use of Artificial Intelligence (AI) is governed by the School's AI Acceptable Use policies for both staff and pupils.

14 Misuse

Any breach of this policy by a member of staff or a pupil will result in appropriate disciplinary action or sanctions.

13 Data Protection

All staff should familiarise themselves with the School's Data Protection and Data Breach policies and its Privacy Notice.

All policies can be found in the relevant Workspace area on Cezanne.