# HAMPTON SCHOOL TRUST

## ESafety Policy

## Contents

**Introduction**
This policy applies to the Hampton School Trust (the Trust), which comprises Hampton School and Hampton Pre-Prep & Prep School (together the School), for children from the Early Years Foundation Stage (EYFS) to the Upper Sixth. The welfare of all pupils is our paramount responsibility. Every adult who works at the School is aware that they have a responsibility for keeping all pupils safe at all times and this includes online safety.

**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. The Trust understands the responsibility to educate pupils about online safety issues, to teach them appropriate behaviours when using the internet and related technologies in and beyond the classroom. It is also committed to establishing a clear set of expectations around the online behaviour of both pupils and staff.

**Safety**
ESafety is the responsibility of the Designated Safeguarding Lead (DSL). At Hampton School the DSL (Owen Morris , Deputy Head (Pastoral)) works closely with the Head of PHSE and ESafety Officer and with Pippa Message (Deputy Head) - one of the Deputy Designated Safeguarding Leads (DDSL), and Deputy Head with responsibility for IT at the Hampton School Trust. At Hampton Pre-Prep & Prep (HPP&P) Tammy Howard, the DSL, has responsibility for online safety. 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 ( click here)

The ESafety Officer, along with the Deputy Heads and Head of Pre-Prep, will review the policy annually as the technological environment changes rapidly.

This policy applies to all members of the Trust's community (including staff, pupils, parents, visitors) who have access to and are users of Trust's IT systems, both in and out of the School. This policy covers both fixed and mobile devices provided by the Trust, as well as devices owned by pupils or staff and brought onto Trust premises. The policy, supported by the other relevant policies listed below, seeks to protect the safety of pupils and staff.

**Other Relevant Policies**
This policy should be read in conjunction with the following Trust policies:

- **Safeguarding Policy** –which makes particular reference to ESafety and the four "areas of risk" outlined in Keeping Children Safe in Education (KCSiE) 2023 - online conduct, contact, conduct and commerce
- Hampton School's **Code of Conduct** and the **Behaviour, Rewards, Sanctions, Discipline and Exclusions Policy** and Hampton Pre-Prep & Prep's **Policy to Promote Good Behaviour – Rewards – Sanctions – Exclusions**
- **Staff ICT Acceptable Use Policy**
- **Anti-Bullying Policy** (which contains particular reference to Cyber-bullying and possible examples of this)
- **Staff Behaviour Policy** (which contains particularly relevant sections on staff communication with pupils, staff internet use, staff use of social networks)
- **Data Incident & Breach Policy**
- **Data Subject Rights Policy**

**Education – Pupils**
Hampton School and HPP&P reinforces internet safety messages to all pupils at regular intervals and at an age-appropriate level through PSHE lessons (Life Skills at HPP&P ), assemblies and by inviting in external organisations/experts to speak to students and share their expertise and up to date knowledge and so supplement lessons delivered by staff. Issues covered include the following:

- safe and appropriate use of social networking sites (specifically age-appropriate);
- the issues surrounding excessive use of games consoles, internet gaming sites, mobile phones (especially texting) and social networking or messaging facilities;
- the sending of inappropriate photos via mobile phone or the internet;
- the dangers of illegal and harmful substances sold online;
- the effect on pupils' wellbeing and self-image of social media and other messages that they may get from online activity;
- the effect of internet pornography on pupils' self-image and their relationships with others
- the dangers of communicating with others online

Members of staff are informed of the **Staff ICT Acceptable Use Policy** which explains their responsibility for safe and appropriate use of the Trust's IT systems.

ESafety should be a focus of all areas of the curriculum and staff should reinforce ESafety messages across the curriculum. The ESafety curriculum should be broad, relevant and provide progression, and will be provided in the following ways:

- An ESafety curriculum is provided as part of PSHE (Life Skills) lessons and is regularly revisited *(see below*).
- Key ESafety messages are reinforced as part of a planned programme of whole school and individual year group assemblies.
- Pupils are taught to be critically aware of the materials and content they access online and be guided to validate the accuracy of information.
- When they join the School, pupils are asked to read and sign a Pupil IT Acceptable Use document 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 with their parents at home.
- Pupils are helped to understand the benefits and risks associated with social media, online posting and messaging.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.

**ESafety Education in PSHE (Life Skills)**
At Hampton School, every form begins the year with a discussion on expectations of behaviour and cyber safety regarding Bring Your Own Device (BYOD) and School supplied iPads and laptops.

ESafety is covered in PSHE lessons in each year group in a structured and age-appropriate way, following a spiral curriculum. Every year the precise nature of these lessons may change, as we continuously update our provision, but consistent themes and messages are reinforced. This includes emphasising pupils are not in control of anything they post online and they need to make responsible choices in their online behaviour. Moreover, there are many dangers and ways they can be taken advantage of online, if they are not careful.

Each year the School ensures that it is able to respond appropriately to any newly identified area of concern within ESafety (e.g. online influencers), and has the capacity to do so within our PSHE (Life Skills) curriculum.

PSHE lessons, where ESafety is specifically addressed at **Hampton School** are listed below:

**First Year (Year 7)**
- DW1.2 Digital Safety: Online dangers and ways to protect yourself.
- RSE1.3 Sex in the Media & Online: Lesson as part of RSE curriculum on Sex and Relationships in the Media including how portrayal of relationships online may not be real
- RSE1.4 RSE talk including information about online portrayal of sex and relationships
- DW1.4 – 1.6 DAUK online courses covering Posture Wellness, Balance & Screens and Hacking are completed by pupils during PSHE lessons on the online platform in the Spring Term

- DW2.1 – 2.3 Pupils prepare and present on an assigned social media platform (TikTok, Instagram, Twitter, Discord, Reddit, Youtube, Whatsapp, Snapchat, BeReal) looking at privacy controls available on those platforms
- DW2.4 Digital Age Limits: reasons for age limits of different types of content online
- RSE2.3 Social Media Technology & You: differences between interacting online and in the real world
- HC 2.2 Lesson on self-esteem considers cyber-related issues
- DW2.5 – 2.8 DAUK online courses on Digital Eye Strain, Sleep & Screens, Scams and Trash Talk & In Game Abuse are completed by pupils during PSHE lessons on the online platform in the Autumn Term

**Third Year (Year 9)**

- RSE Course Cyber related issues covered extensively in RSE programme (focus on sexting and sharing of indecent images)
- DW3.1 – 3.3 DAUK online courses on Digital Footprint, Online Hate Speech and Sexting & Consent are completed by pupils during PSHE lessons on the online platform

**Fourth Year (Year 10)**

DW4.1 Making the most of social media: Discussing opportunities available on social media and how it can be used positively

- DW4.2 Privacy on Social Media: Importance of privacy policies and how data is collected
- DW4.3 Gaming and Gambling talk with follow up discussions in class

**Fifth Year (Year 11)**

DW5.1 Social Media in Society: wider impact of social media including fake news, election advertising and hate speech with case study examples

DW5.2 Artificial Intelligence Talk

**Lower Sixth (Year 12)**

DW6.1 Echo Chambers on Social Media: know how to leave an echo chamber and impact of them on society

DW6.2 Topical discussion on a current online development e.g. Elon Musk taking over Twitter, ChatGPT, Online Safety Bill

**Upper Sixth (Year 13)**

DW7.1 Professionalism on Social Media: how to contribute to your career prospects e.g. use of LinkedIn profiles

DW7.2 Digital Law: focussing on laws surrounding upskirting, libel/slander sexting, revenge porn and how the law changes at age 18

DW7.3 Digital Commerce: recall common scams and how to earn an income online

This is also specifically addressed in Life Skills lessons at **Hampton Pre-Prep & Prep School** at the following times:

- EYFS – Information about online safety is delivered at an age appropriate level as part of Personal, Social and Emotional Development and Understanding the World (Digiduck's Big Decision).

- Pre-Prep pupils in Years 1 and 2 receive regular reminders about keeping safe online.

- From Reception to Year 6, pupils follow the Jigsaw programme as part of the Life Skills and Relationships Education programme.

- From Year 3, this specifically includes the following:
    - Keeping safe and why it's important online and offline
    - Keeping safe online and where to go for help

- Year 4
    - Being a school citizen
    - Understanding influences

- Year 5
    - Rights and responsibilities online
    - Online gaming and gambling
    - Reducing screen time
    - Dangers of online grooming
    - SMARRT internet safety rules

- Year 6
    - Technology safety
    - Take responsibility with technology use
    - Sexting

In addition to this, Year 6 take part in the Leavers' Programme, which includes a talk by various professionals, including key messages about safety and safe use of mobile phones.

Safer Internet Day is supported annually at the School. Providers, such as Openview Education and Childnet also deliver age appropriate internet safety talks to pupils in Reception – Year 5.

Online Safety matters are also addressed in ICT lessons throughout the year and across all year groups. Resources from Purple Mash and Espresso are used to support the delivery of these lessons.

**Education – Parents**
Parents play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviour.

Advice on cyber safety and cyber issues is given to parents from time-to-time at Year Group Pastoral Forums for parents, at Parents' Evenings and on other occasions.

This advice is drawn from recommendations made by CEOP (Child Exploitation and Online Protection Centre):

- Make yourself aware of the amount of time your child is using the internet, chat facilities, games consoles and their mobile phones and whether this is excessive
- Consider carefully the location of the computer or laptop and whether your child would be better using it in a family area of the home
- Search on Google and other search engines for your child's name and any online usernames they use. This is a valuable exercise for you and them to see exactly how much other people can see about them with very little difficulty
- Consider installing internet monitoring software on home computers
- Talk to your child; both about the dangers or the internet, but also about their general usage – be interested in what they are doing and keep a dialogue open so they feel able to talk to you if they do experience problems
- Ask your child to (or help them) set up appropriate privacy settings on Facebook (please contact the School if you need help or advice in this area)

**Parents' Talks and Intranet provision**
At **Hampton School,** external speakers come in to talk to parents each year. Peter Cowley delivers an ESafety webinar in the Autumn Term for parents of pupils in 1st – 5th year.

Digital Awareness UK deliver a parent webinar in the Summer Term for all parents of pupils in 1st-3rd year.

As well as these dedicated events, the ESafety Officer speaks to parents as part of different 'Pastoral Forums' – these are Meet the Tutor evenings that happen in all year groups at the start of the year (these are not joint with LEH).

The DDSL and ESafety Officer also communicate with parents as issues arise with advice via email.

Similarly, at HPP&P external speakers (e.g. OpenView / Childnet come in to talk to parents and all parents are invited to attend.

**A termly safeguarding letter is sent to parents outlining local and national issues pertinent to safeguarding. The School also regularly sends out guidance from the local authority on setting parental restrictions on devices at home.**

**Education and Training – Staff**
Staff receive training on INSET days as well as updates during Hampton School's Tuesday briefings (and Hampton Pre-Prep & Prep's staff meetings) on IT and E-Safety issues. Firefly contains further advice. The **Staff Behaviour Policy** and **Staff Handbook** also contain sections with advice on staff communication with pupils, staff internet use and staff use of social networks.

All staff complete an Online ESafety course (either the NSPCC course, or the equivalent *Educare* module) and a Digital Awareness course. In addition, elements of ESafety training regularly feature in staff safeguarding updates.

**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 **IT Acceptable Use Policy** that all pupils are required to sign. The Trust's rules and disciplinary procedures associated with the misuse of devices, digital technology and the network are explained in the Hampton **School Code of Conduct** and the **Behaviour, Rewards, Sanctions, Discipline and Exclusions Policy (**at Hampton Pre-Prep and Prep**,** the **Policy to Promote Good Behaviour – Rewards – Sanctions – Exclusions)**

**Confiscation and Searching of pupil devices:** an electronic device such as a mobile phone or a tablet computer may be confiscated in appropriate circumstances in accordance with **the Behaviour, Rewards, Sanctions, Discipline Exclusions Policy**. If there is good reason to suspect that the device has been, or could be used to cause harm, to disrupt teaching or break school rules, any data or files on the device may be searched and, where appropriate, data or files may be erased before the device is returned to its owner.

The expectations of staff for using the internet, email and other forms of digital technology are set out in the **Staff Behaviour Policy**.

**Filtering and Monitoring**
As part of its Safeguarding duty, the Trust has put in place filtering and monitoring to try to ensure children are safe when accessing the internet in school. The Trust's network uses filtering software for all website activity, and appropriate age restrictions applied. The Safeguarding team receives reports on staff and pupil use of the School's network and online activity. In addition, the Trust has safeguarding screen-capture software that records monitors key phrases and images to ensure content accessed via the School network is appropriate.

More information on the School's filter and monitoring procedures can be found in the **Safeguarding Policy** which is available to all staff in the in the Documents area in the relevant Workspace on Cezanne (see link above).

**Behaviour and Anti-Bullying**
Cyberbullying by pupils will be treated as seriously as any other type of bullying, and will be managed through our anti-bullying procedures, and they can be escalated to safeguarding concerns.

The appropriate School disciplinary procedures are followed in relation to any incident of misuse of ICT equipment or websites or of cyber bullying. The School reserves the right to take action - even when the offence is committed outside of School - if it harms members of our community or brings the School into disrepute.

Cyber bullying is an aggressive, intentional act carried out by a group or individual, using electronic forms of contact, against a victim who cannot easily defend him/herself. It is sometimes also known as 'online abuse' as the term cyber-bullying can become trivialised through overuse. Mobile, internet and wireless technologies have increased the pace of communication and brought benefits to users worldwide. Unfortunately, however, their popularity provides the opportunity for misuse through cyber bullying.

Cyber bullying includes: Text message bullying; picture/video bullying via mobile phone cameras; phone call bullying via mobile phone; email bullying; chat room or social network bullying; bullying through instant messaging; bullying via websites; bullying via gaming platforms.

*Ways pupils can keep themselves and others safe include:*

- Not posting personal items (including photographs) or information– keep information general.
- Thinking carefully about posting pictures online – once it is there, anyone can see it or use it.
- Not sharing passwords –personal information should be kept private
- Never meeting up with someone they have 'met' online without a responsible adult being present.
- Thinking carefully before writing anything online – people can misinterpret words.
- Respecting other people's views – there is no need to be rude or abusive if opinions differ.

*What can a pupil do if they a victim of cyber bullying:*

- Tell someone they trust.
- Report any cyberbullying, even if it is not happening to them.
- Never respond/retaliate as it could make matters worse.
- Block the cyberbullies.
- Save and print any bullying messages, posts, pictures or videos that are received or seen online so that they can be passed on to the School or other authorities, should this be required. Make a note of the dates and times they are received.

Sexting and revenge porn are taken particularly seriously and boys are educated about the dangers and possible consequences of these acts through PSHE lessons.

Cyber bullying is explicitly referred to in both schools' **Anti-Bullying Policy***.
*HPP&P has its own Anti-Bullying policy.

The expectations of Hampton School pupils in this area are clearly set out in the **School Code of Conduct**, which is printed each term in every pupil's yellow School calendar. School Assemblies and PHSE lessons are also used to update pupils on relevant cyber issues.

**Youth produced sexual or indecent imagery**
Indecent imagery is the legal term used to define nude or semi-nude images, videos or live streams of children and young people under the age of 18. This could be via social media, gaming platforms, chat apps or forms. Consensual and non-consensual sharing of nude images and/or videos can be signs that children are at risk.

Consensual image sharing, especially between older children of the same age, may require a different response. It might not be abusive - but children still need to know it is illegal - whilst non-consensual is illegal and abusive. The School follows the guidance given by the *UKCIS Sharing nudes and semi-nudes: advice for education settings working with children and young people*.

The School treats all incidences of sexting as safeguarding matters to be actioned in accordance with the School's **Safeguarding Policy**. The School's sanction system will also be used depending on circumstances (refer to the **School Code of Conduct** and the **Behaviour, Sanctions, Rewards, Discipline and Exclusions**

**Policy*** which refer to sexual misconduct and the possession and supply of indecent imagery).
*Hampton Pre-Prep & Prep School has its own policy - **Promote Good Behaviour – Rewards – Sanctions - Exclusions**

**ESafety: Safeguarding and "Prevent"**
Some adults and young people may use technologies to harm children and the School is are aware of the Safeguarding concerns linked to ESafety. *KCSiE 202*3outlines four areas of risk:

(i) online content (being exposed to harmful material);
(ii) contact (being subjected to harmful interaction with others online);
(iii) conduct (personal online behaviour that increase the likelihood of, or causes, harm); and
(iv) commerce – risks such as online gambling, inappropriate advertising, phishing or financial scams.

When necessary, the Trust will inform the police or Achieving for Children (Richmond and Kingston) if they have concerns about the online activities of pupils at the School.

The Counter-Terrorism and Security Act 2015 places a duty on specified authorities, including Schools, to have due regard to the need to prevent people from being drawn into terrorism ("the Prevent duty"). As part of the Trust's "Prevent duty" the issue of extremist or terrorist material on the internet is covered in PSHE lessons. The Trust's filtering and monitoring software ensures children are safe from accessing terrorist or extremist material when using the internet in School. The Trust's **Safeguarding Policy** explains in more detail how Hampton School and HPP&P address these issues.