HAMPTON SCHOOL TRUST

ESafety Policy

Contents

Date updated	December 2024	Date ratified by Governors	December 2024
Date of next review	December 2025	Reason for Review	Annual Review

Introduction

This policy applies to all schools within the Hampton School Trust (the Trust or the School), for children from the Early Years Foundation Stage (EYFS) to the Upper Sixth. The welfare of all pupils is the School's 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.

The 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. It covers both fixed and mobile devices provided by the Trust, as well as devices owned by pupils or staff 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.

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, including but not limited to bullying, harassment, grooming, stalking, abuse, radicalisation, how to best mitigate risks and what to do should they come across something of concern. This is done through providing pupils with the critical thinking skills necessary to use technology to their advantage and teaching them appropriate behaviours when using the internet and related technologies in and beyond the classroom whilst keeping them safe and operating within the law. Current and emerging technologies used in and outside of school include: Websites, Emails and instant messaging, Blogs/Vlogs, Social Media sites, Music/video downloads, Gaming sites, Text and picture messages, Video calls, Podcasting, Applications, Online communities, Artificial Intelligence, Virtual and augmented reality technology. The School is also committed to establishing a clear set of expectations around the online behaviour of both pupils and staff.

Safety Responsibilities

Hampton School

ESafety 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 and ESafety Officer, and with Pippa Message (Deputy Head) – a DDSL and Deputy Head with responsibility for IT at the Hampton School Trust.

Hampton Pre-Prep & Prep

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

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 (click here)

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

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**
- **Data Incident & Breach Policy**
- **Data Subject Rights Policy**
- 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 (inc. Rewards – Sanctions – Exclusions)**

- **Safeguarding Policy** –which makes particular reference to ESafety and the four “areas of risk” outlined in Keeping Children Safe in Education (KCSiE) 2024 - online conduct, contact, conduct and commerce
- **Staff Behaviour Policy** (which contains particularly relevant sections on staff communication with pupils, staff internet use, staff use of social networks)
- **Staff ICT Acceptable Use Policy**

Education – Pupils

Upon 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, they are told not to use them). 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 reinforced 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 both pupils and staff are made aware of this. As technology continues to develop, IT and the use of the internet is being increasingly used across all aspects of the curriculum in all years. Therefore, Hampton School and HPP&P reinforces internet meaningful ESafety guidance to pupils regularly at an age-appropriate level in different settings 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 supplementing lessons delivered by staff in addition to when informal opportunities arise. 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;
- recognising online scams and phishing attempts
- 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
- critically analysing information online to identify fake news, deepfakes and echo chambers

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 is a focus of all areas of the curriculum and staff regularly reinforce ESafety messages across the curriculum. The ESafety curriculum is broad, relevant and provides 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. 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 the attached form and all responses are tracked.

- 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, safeguarding and cyber safety regarding Bring Your Own Device (BYOD) and School supplied laptops.

ESafety is covered mainly through the Digital Wellbeing Strand 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 once it has been posted 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, Deepfake technology), and has the capacity to do so within our PSHE (Life Skills) curriculum through our Living in the Wider World strand and topical discussion sessions.

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

First Year (Year 7)

- DW1.1 Digital Skills: Learning how to use digital equipment appropriately
- DW1.2 Digital Safety: Online dangers and ways to protect yourself
- RSE1.4 RSE talk including information about online portrayal of sex and relationships
- DW1.4 Posture Wellness
- DW1.5 Hacking
- DW1.6 Balance and Screens

Second Year (Year 8)

- RSE2.9 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
- DW2.1 – 2.3 Introduction to Social Media: 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: a peer delivered lesson looking at the differences between interacting online and in the real world
- HC 2.2 Self-Esteem: Lesson on self-esteem considers cyber-related issues
- DW2.5 Trash Talk & In-Game Abuse: pupils identify different types of in-game abuse and discuss coping strategies for managing abuse online
- DW2.6 Sleep and Screens: importance of sleep and how technology can impact this
- DW2.7 Scams: different types of scams, relevant terminology, preventing themselves from being scammed and what to do if they have been scammed
- DW2.8 Digital Eye Strain: impact of screens on our eyes and how to prevent it

Third Year (Year 9)

- All new joiners are updated on lessons from First and Second Year on New Boys Morning to prevent and gaps in knowledge, the main focus being staying safe online
- RSE Course Cyber related issues covered extensively in RSE programme (focus on sexting and sharing of indecent images) (see RSE Policy for further details)
- DW3.1 Digital Footprint: enabling pupils to make informed decisions about what information they share online

- DW3.2 Online Hate Speech: reminder about protected characteristics and the laws surrounding hate speech
- DW3.3 Sexting and Consent: what sexting is and how to get support
- DW3.4 Scenarios: online scenarios they may encounter are discussed e.g. bullying, online harassment, trash talk
- DW3.5 Social Media Discussion: a discussion about what pupils like/dislike about social media and how it makes them feel

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 and the development of AI, 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
- DW7.4 18+ Internet: discussion about the parts of the internet that officially become available at 18 (e.g. gambling, dating aps)
- DW7.5 Topical Discussion on a current online development e.g. Elon Musk taking over Twitter, ChatGPT and the development of AI, Online Safety Bill
- DW7.6 AI in the Future Talk

ESafety is also specifically addressed in Life Skills and Computing 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
    - Digital awareness

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

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

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.

HPP&P also celebrates Safer Internet day each year with whole school events over the week.

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. A speaker from Achieving for Children delivers an ESafety webinar in the Spring Term for parents of pupils in 1st – 5th 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

The DDSL, Heads of Year and ESafety Officer also communicate via email with parents, giving advice as issues arise

At Hampton School, 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.

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.

Education and Training – Staff

Staff receive training on INSET days as well as session specific training for upcoming PSHE lessons where more in depth knowledge is needed for the session and updates are given during Hampton School's Tuesday briefings (and Hampton Pre-Prep & Prep's staff meetings) on IT and E-Safety issues. SharePoint 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 (including artificial intelligence) 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 (inc. 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 pupils are safe when accessing the internet in school. Reviews of which websites are appropriate for pupils and staff to access are undertaken regularly and added to the filtering system. 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.

The Trust's network uses filtering software for all website activity, and appropriate age restrictions applied. 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 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 and conversations are had with the relevant pupils. 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 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; bullying by picture/video manipulation through the use of editing software/artificial intelligence; 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.
- Not engaging in image/video manipulation that can cause harm to others

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.

All of these messages are reinforced through the Digital Wellbeing strand of our PSHE curriculum.

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. At HPP&P, expectations are set out in the School Code.

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 aware of the Safeguarding concerns linked to ESafety. *KCSiE 202*4 outlines 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.