Hampstead Hill School

Respect. Kindness. Community. Curiosity. Conservation.

Online Safety Policy

Table of Contents

1. Aims

Hampstead Hill School aims to:

- Have robust processes in place to ensure the online safety of pupils, staff and volunteers
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and Guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Searching, screening and confiscation

It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy should be read in conjunction with the Computing Skills Progression Map and Computing plans in the Upper School.

3. Roles and Responsibilities

3.1 The Directors

The Directors have overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The Directors will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).

All Directors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on Acceptable Use of the school's ICT systems and the internet
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable pupils, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all pupils in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The Headteacher

The Headteacher has overall responsibility for monitoring this policy and ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Lead

Details of the school's DSL and deputies are set out in our Child Protection and Safeguarding Policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Headteacher, Head of Lower School, Computing Lead, IT Manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Headteacher

3.4 The IT manager

The IT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Working with the Headteacher or Head of Upper School to ensure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

3.5 All Staff and Volunteers

All staff, including agency staff and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently

- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendices 1)
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

3.6 Parents

Parents are expected to:

- Notify a member of staff, the Head of Upper School or the Headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (see appendices 1)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International

Please see the Anti-Buying Policy for further guidance.

4. Pupils with Special Needs

Pupils with learning difficulties or disabilities may be more vulnerable to risk from use of the internet and may need additional guidance on e-safety practice as well as closer supervision.

SENDCO is responsible for providing extra support for these pupils and should:

- link with the Heads of Year to discuss and agree whether the mainstream safeguarding systems on the internet are adequate for pupils with special needs
- where necessary, liaise with the IT Manager to discuss any requirements for further safeguards to the school IT system or tailored resources and materials in order to meet the needs of pupils with special needs
- ensure that the school's e-safety policy is adapted to suit the needs of pupils with special needs
- liaise with parents and other relevant agencies in developing e-safety practices for pupils with special needs
- keep up to date with any developments regarding emerging technologies and e-safety and how these may impact on pupils with special needs.

5. Educating Pupils About Online Safety

The widespread use of digital communications technologies, such as personal mobile devices and the internet, presents pupils with a host of opportunities for learning, participation, creativity and self-expression. At the same time, it allows them to access and transmit harmful content along with being

a means to harass and bully their peers. The School recognises that some pupils, could potentially use digital devices to bully, control or harass others, or view harmful content.

Many children now have unrestricted access to the internet, which some of them may abuse to sexually harass their peers, share indecent images consensually and non-consensually and view and share harmful content. Hampstead Hill School employs a range of strategies to promote an understanding of online risks and to discourage misuse.

In the Upper School, pupils will be taught to:

- Exploring e-safety in detail via the curriculum and pastoral events
- Ensuring systems are in place to facilitate early disclosure of potentially harmful online incidents
- Providing information to parents about how the school uses filters and monitors online use and, more generally, to promote understanding of the varied and evolving nature of online risks
- Informing pupils (and their parents) of the online activity that will be expected of them as members of the school: the websites they will be expected to access (eg, iSAMS); and how and with whom they will interact online
- Deterrence through the use of robust sanctions against those found to have abused others online

The safe use of social media and the internet will also be covered in PSHE and Computing.

HHS understand the importance of equipping pupils to stay safe online in school and outside. We use our Computing curriculum and E-Safety week to educate pupils and parents on preventing radicalisation while engaging in online activity.

HHS uses PSHE assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

In the Lower School:

- Pupils will be taught to use the internet safely. Teachers will show and discuss child friendly 'EYFS online safety' ppt.
- Staff will regularly talk about online safety and remind pupils to ask an adult at home when they want to use devices or access the internet.
- Staff will role model safe behaviour and privacy awareness.
- Staff will check the content and suitability of the internet sites they will show to the pupils.

6. 4C's Classification

Though the age and developmental stage of our pupils may mean they are not exposed to certain online risks, we acknowledge the opportunity and possibility and follow the '4C's' classification of areas of risk regarding online safety.

1. **Content**: Being exposed to illegal, inappropriate or harmful online content such as spam, pornography, fake news, substance abuse, violence, misogyny, anti-Semitism, racism, radicalisation and extremism, and lifestyle sites that promote anorexia, self-harm or suicide.
2. **Contact**: Being subjected to harmful online interaction with other users. Examples include: child to child pressure, exposure to viruses and malware, anonymous online chat sites, cyber-bullying commercial advertising, personal data or identity theft, cyber-stalking, and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

3. **Conduct**: Personal online behaviour that increases the likelihood of being harmed oneself or causing harm to others. Examples include: threats to health and wellbeing, such as gaming or social network addiction; online disclosure of personal information and ignorance of privacy settings; online bullying; making, sending and receiving explicit images (eg consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images); and illegal conduct, including hacking, plagiarism, and copyright infringement of digital media, such as music and film.
4. **Commerce**: Risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

7. Educating Parents About Online Safety

HHS will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the head of Upper School, the Headteacher and/or the DSL.

8. Cyber-Bullying

7.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

The school will adopt a zero-tolerance approach to any cyber bullying issues. All staff will challenge any abusive behaviour between peers that comes to their notice and will report on to the DSL immediately any issues of this nature. See the Safeguarding Policy for further details about dealing with child-on-child abuse.

7.2 Preventing and addressing cyber-bullying

Pupils are not left on their own on devices in school and due to the age of our pupils, we expect them to be supervised when online at home. HHS strongly encourages parents not to allow pupils to spend significant amounts of time online or on IT devices.

To help prevent cyber-bullying, we ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

HHS discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. This is included in both the PSHE and Computing curricula as well as specific events such as Safer Internet Day.

All staff receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the Anti-Bullying Policy.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

9. Acceptable use of the Internet in School

All pupils, parents and staff (volunteers and visitors if applicable) are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1).

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

The IT Manager will monitor the websites visited by pupils, staff, volunteers and visitors (where relevant) to ensure they comply with the above.

10. Pupils Using Mobile Devices in School

Due to the age of our pupils, they do not bring mobile devices to school.

11. Staff Using Work Devices Outside School

Staff using a work device outside school must follow the Acceptable Use Policy

Staff must sign out their device with the IT Manager if they are taking off the premises.

12. How the School Will Respond to Issues of Misuse

Pupils are supervised when using IT devices or the internet – where a pupil misuses the school's devices or the internet, action will be taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member fails to comply with Acceptable Use Policy Agreement, he/she could be subject to disciplinary action as per the terms laid out in the school's Disciplinary Policy.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

13. Training

All new staff members will receive training as part of their induction on safe internet use, online safeguarding issues including cyber-bullying, peer on peer abuse and the risks of online radicalisation.

All staff members will receive refresher training at least once every other academic year as part of safeguarding training, as well as relevant updates as required (for example through emails and staff meetings).

The DSLs will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals.

Volunteers will receive appropriate training and updates, if applicable.

14. Monitoring Arrangements

Staff reports and log behaviour and safeguarding issues related to online safety on CPOMS.

This policy will be reviewed every year by the DSL. At every review, the policy will be shared with the Headteacher and Directors. The review will consider new risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

15. Links with other policies

This online safety policy is linked to our:

- Child protection and Safeguarding Policy
- Behaviour Policy
- Staff Disciplinary Procedures
- Data Protection Policy and Privacy Notices
- Complaints Procedure
- Acceptable Use Policy

Dates Reviewed	January 2024
Next Review	January 2025
Name	 Anne Napier Headteacher

Appendix 1: EYFS and KS1 Acceptable use Agreement (pupils and parents/carers)

<table>
<tr><td colspan="2">ACCEPTABLE USE OF HHS' ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS</td></tr>
<tr><td colspan="2">Name of pupil:</td></tr>
<tr><td colspan="2">When I use the HHS ICT systems (like computers) and get onto the internet in school I will:
Ask a teacher or adult if I can do so before using them
Only use websites that a teacher or adult has told me or allowed me to use
Tell my teacher immediately if:
I click on a website by mistake
I find anything that may upset or harm me or my friends
Use school computers for school work only
I will be kind to others and not upset or be rude to them
Look after the school IT equipment and tell a teacher straight away if something is broken or not working properly
Only use the username and password I have been given
Try my hardest to remember my username and password
Never share my password with anyone, including my friends.
Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
Save my work on the school computer
Check with my teacher before I print anything
Shut down a computer when I have finished using it
I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.</td></tr>
<tr><td>Signed (pupil):</td><td>Date:</td></tr>
<tr><td colspan="2">Parent/carer agreement: I agree that my child can use the HHS' IT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using HHS' ICT systems and internet and will make sure my child understands these.</td></tr>
<tr><td>Signed (parent/carer):</td><td>Date:</td></tr>
</table>