HURLINGHAM SCHOOL
AND NURSERY
EST. 1947

E-Safety Policy

This policy applies to all activities of Hurlingham School, including the Early Years Foundation Stage.

Date of Review: September 2024
Date of Next Review: by 31 May 2025

Contents:

1. Introduction

It is our duty to ensure that every pupil in our care is safe; and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle risks to young people. 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 identity theft, bullying, harassment, grooming, stalking, abuse and radicalisation.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used in and outside of school include:

- Websites;
- Email and instant messaging;
- Blogs;
- Social networking sites;
- Music / video downloads;
- Gaming sites;
- Text messaging and picture messaging;
- Video calls;
- Podcasting;
- Online communities via games consoles; and
- Internet enabled devices such as smartphones and tablets.

We understand that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content:** Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.
- **Contact:** Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.
- **Conduct:** Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- **Commerce:** Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. We have created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

2. Legal Framework

2.1 This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2024) ‘Filtering and monitoring standards for schools and colleges’

- DfE (2021) ‘Harmful online challenges and online hoaxes’
- DfE (2024) ‘Keeping children safe in education 2024’
- DfE (2023) ‘Teaching online safety in school’
- DfE (2022) ‘Searching, screening and confiscation’
- DfE (2023) ‘Generative artificial intelligence in education’
- Department for Science, Innovation and Technology and UK Council for Internet Safety (2024) ‘Sharing nudes and semi-nudes: advice for education settings working with children and young people’
- UK Council for Child Internet Safety (2020) ‘Education for a Connected World – 2020 edition’
- National Cyber Security Centre (2020) ‘Small Business Guide: Cyber Security’

2.2 This policy operates in conjunction with the following school policies:

- Staff Acceptable Use Policy and Agreement;
- Pupil Acceptable Use Policy and Agreement (Safe and Sensible Computing agreement);
- Mobile Device Policy for Staff, Pupils, Parents and Visitors;
- Social Media Policy; and
- Taking, Storing and Using Images of Children Policy
- Remote Learning Policy.

It is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is also linked to the following school policies:

- Privacy Notice;
- Safeguarding and Child Protection Policy;
- Staff Code of Conduct;
- Health and Safety Policy;
- Promoting Positive Relationships and Supporting Behaviour Regulation Policy;
- Anti-Bullying Policy;
- Data Protection Policy;
- PSHEE and Citizenship Policy;
- Disciplinary Policy and Procedures; and
- Confidentiality requirements contained with staff employment contracts.

Whilst exciting and beneficial both in and out of the context of education, much IT, particularly online resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

At Hurlingham, we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving pupils in discussions about e-safety and listening to their fears and anxieties as well as their thoughts and ideas.

The DSL takes lead responsibility for safeguarding and child protection including online safety and understanding the filtering and monitoring systems and processes in place. All e-safety incidents should be reported to the DSL and Mikaela Elbourne, the Head of Digital Strategy and Computing and where appropriate, the Head of IT Services and the Head unless any of the above are the subject of the concern.

3. Scope of this Policy

This policy applies to all members of the school community, including staff, pupils, parents and visitors, who have access to and are users of the school IT systems. In this policy:

- 'staff' includes teaching and non-teaching staff, Advisors, and regular volunteers;
- ‘Parents’ includes pupils' carers and guardians;
- 'Visitors' includes anyone else who comes to the school, including occasional volunteers.

This policy covers both fixed and mobile internet devices provided by the school (such as PCs, laptops, tablets, whiteboards, visualisers, digital video equipment, etc.); as well as all devices owned by pupils, staff, or visitors and brought onto school premises (personal laptops, tablets, smart phones, etc.).

4. Roles and responsibilities

The Board of Directors of the school is responsible for the approval of this policy and for reviewing its effectiveness. This policy will be reviewed (at least) annually and the Principal is responsible for keeping the Board of Directors and Board of Advisors fully informed about the School’s procedures in relation to e-safety.

Fiona Goulden, Principal, is the named member of the Board of Directors with responsibility for Safeguarding, which includes e-safety. This role involves meeting with the E-safety Officer, reviewing the details of e-safety incidents and reporting to the relevant Board level meetings.

The Head is responsible for the safety of the members of the school community and this includes responsibility for e-safety, although day-to-day responsibility for e-safety will be delegated to the E-Safety Officer.

In particular, the role of the Head (and the Senior Leadership) team is to ensure that:

- staff, in particular the DSL, E-Safety Officer, the Head of PSHEE and the Head of IT Services are adequately trained about e-safety; and
- staff are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of e-safety in connection to the school.

The DSL is responsible for:

- Taking the lead responsibility for online safety in the school.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT technicians.
- Ensuring online safety is recognised as part of the school’s safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school’s approach to remote learning.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure.
- Understanding the filtering and monitoring processes in place at the school.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.
- Maintaining detailed, secure and accurate written records of reported online safety concerns as well as the decisions and whether or not referrals have been made.
- Understanding the purpose of record keeping.

- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Reporting to the Principal about online safety on a termly basis.
- Working with the Head and ICT technicians to conduct termly light-touch reviews of this policy.
- Working with the Head and Principal to update this policy on an annual basis.

The E-Safety Officer is responsible for:

- monitoring student use of internet and devices, in conjunction with the Head of IT Services and the DSL;
- dealing with e-safety incidents (in conjunction with the DSL, Head, Head of IT Services and the Head of PSHEE), where relevant, in accordance with the School's Safeguarding and Child Protection Policy;
- ensuring that staff are aware of the procedures and policies that should be followed in the event of an e-safety incident taking place;
- taking day-to-day responsibility for e-safety issues and reviewing the School's e-safety policies;
- arranging for training and advice to be provided for staff, pupils and parents in collaboration with the Head of PSHEE and the DSL;
- maintaining a record on the CPOMS system of any e-safety incidents and any subsequent investigations and ensuring that members of staff enter details of any e-safety concerns on the same;
- using the e-safety log on CPOMS to identify and track concerns and patterns to inform the School's procedure and policy reviews;
- ensuring that the Head and DSL receive incident alerts via CPOMS relating to any e-safety concerns;
- meeting with the Head and DSL to report on current issues, following termly reviews;
- liaising with the DSL to follow up any safeguarding issues that may arise from:
    - Access to illegal or inappropriate materials;
    - Inappropriate online contact with adults /strangers;
    - Potential or actual incidents of grooming;
    - Cyber-bullying (see the Anti-Bullying Policy).

The Head of IT Services is responsible for:

- monitoring the use of the internet and emails;
- maintaining and updating content filters on a regular basis;
- maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments;
- the security of the school's hardware system, its data and for training the school's teaching and administrative staff in the use of IT;
- ensuring that only authorised users are able to access the School's networks and devices;
- reporting the details of any investigations into e-safety incidents to the E-Safety Officer;
- ensuring that the School's antivirus system definitions and web filter categories are updated automatically.

The Head of PSHEE is responsible for:

- ensuring that age appropriate e-safety content is included for all pupils as part of the PSHEE curriculum;
- collaborate with the Head of Digital Strategy and Computing to monitor the provision of e-safety teaching and update the curriculum materials accordingly.
- collaborate with the Head of Digital Strategy and Computing to help parents to understand e-safety issues through arranging parents' information evenings and providing newsletters and information about e-safety campaigns and literature.

Teaching and support staff are responsible for ensuring that:

- they have read, understood and signed the Staff Acceptable Use Policy and Agreement, before accessing the school's systems;
- they have an up-to-date understanding about e-safety matters and have read and understood all of the School's associated policies;
- they report any e-safety concerns to the E-Safety Officer and log any concerns in the School's CPOMS system ensuring that the DSL is also notified if there is any associated safeguarding concern;
- they are professional in all digital communications and that only official school platforms are used for this purpose;
- they help pupils to understand and adhere to the Safe and Sensible Computing Agreement and, as with all issues of safety at this school, staff are encouraged to create a talking and listening culture in order to address any e-safety issues which may arise in classrooms on a daily basis;
- they monitor the use of all digital technologies by pupils in School;
- they check that any online material being shared with the children is suitable and from a reputable source and ensure that pupils are only directed to sites which are suitable for use by children. Any inappropriate content must be reported to the E-safety Officer and the Head of IT Services.

All pupils:

- are responsible for using the school IT systems in accordance with the Pupil Acceptable Use Policy (Safe and Sensible Computing), and for letting staff know if they see IT systems being misused;
- from Year 1 upwards are required to sign the Safe and Sensible Computing Policy before accessing the School's systems or engaging in any remote online provision;
- only access the school network and devices using their own unique login and password;
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do this;
- need to understand the importance of good e-safety practice when using digital technologies both in and out of School.

Parents

Hurlingham School believes that it is essential for parents to be fully involved with promoting e-safety both in and outside of school. We regularly consult and discuss e-safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage. The school will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

Parents are responsible for endorsing the school's Safe and Sensible Computing Agreement and for agreeing to and overseeing the School's protocols for pupils during any period of remote learning.

Parents are responsible for adhering to the School's Mobile Devices Policy.

5. Education and training

Staff: awareness and training

New staff receive information on our E-safety and associated policies as part of their induction.

All teaching staff receive regular information and training on e-safety issues in the form of INSET training and internal meeting time and are made aware of their individual responsibilities relating to the safeguarding of children within the context of e-safety. All teaching staff undertake regular e-safety training delivered by an external provider. The Principal has overall responsibility for online safety and has been trained at the appropriate level for this role as have the E-Safety Officer and the Head of PSHEE.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school e-safety procedures. These behaviours are summarised in the Staff Acceptable Use Policy and Agreement which must be signed and returned before use of technologies in school. When children use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's IT guidelines when signing the Safe and Sensible Computing Agreement.

Teaching staff are encouraged to incorporate e-safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community.

The Head of Digital Strategy and Computing and the Head of PSHEE monitor the provision of e-safety teaching and update the curriculum materials accordingly.

An incident report must be completed by staff as soon as possible on the School's CPOMS platform if any incident relating to e-safety occurs and this must be shared with the E-Safety Officer, the Head and the DSL.

The DSL will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

Pupils: E-Safety in the curriculum

IT and online resources are used increasingly across the curriculum. We believe it is essential for e-safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote e-safety and regularly monitor and assess our pupils' understanding of it. The e-safety curriculum is designed to be broad, relevant and provide progression and will be delivered in the following ways:

- The school provides opportunities to teach about e-safety within a range of curriculum areas and IT lessons. Educating pupils on the dangers of technologies that may be encountered outside school will also be carried out as part of the Computing and PSHEE curriculums, by presentations in assemblies, as well as informally when opportunities arise.
- Pupils are taught:
    - how to evaluate what they see online;
    - how to recognise techniques used for persuasion;
    - acceptable and unacceptable online behaviour and relationships;
    - how to identify online risks;
    - how and when to seek support;
    - online media literacy strategies;
    - how to identify when something is deliberately deceitful or harmful;
    - how to recognise when something they are being asked to do puts them at risk or is age-inappropriate.
- At age-appropriate levels, and usually via PSHEE and Computing, pupils are taught about their e-safety responsibilities to use technology safely, responsibility, respectfully and securely and to look after their own online safety. From Year 5, pupils are formally taught about recognising online sexual exploitation, stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across. Pupils are taught where they can seek help and support if they have

concerns about what they see online and can report concerns to the Head and any member of staff at the school.
- In the Upper School, pupils are also taught about relevant laws applicable to using the internet; such as data protection and intellectual property. Pupils are taught about respecting other people's information and images (etc.) through discussion and classroom activities.
- In addition, the school will implement a cyber awareness plan for pupils and staff to ensure that they understand the basics of cyber security and protecting themselves from cyber-crime.
- The school will implement its cyber security strategy in line with the DfE's 'Cyber security standards for schools and colleges' and the Cyber Security Policy.

Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Anti-bullying Policy, which describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying). Pupils should approach the Head of Digital Strategy and Computing, Head of PSHEE, Head, Head of Section or Principal as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

Parents

The school seeks to work closely with parents to promote a culture of e-safety. The school will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

The school recognises that not all parents and guardians may feel equipped to protect their child when they use electronic equipment at home. The school therefore includes e-safety information in the start of year Welcome Evenings and arranges at least one discussion evenings for parents each year when either the E-Safety Officer or an outside specialist advises about e-safety and the practical steps that parents can take to minimise the potential dangers to their children without curbing their natural enthusiasm and curiosity.

6. Policy Statements

Use of school and personal devices

Staff

School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. Staff should only use the school device which is allocated to them for schoolwork. When they are not using a device staff should ensure that it is locked to prevent unauthorised access. Devices issued to staff are encrypted, to protect data stored on them.

Staff are referred to the Mobile Devices Policy for Staff and Visitors for further guidance on the use of non-school owned electronic devices for work purposes.

Personal telephone numbers, email addresses, or other contact details may not be shared with pupils or parents and under no circumstances may staff contact a pupil or parent using a personal telephone number, email address, social media, or other messaging system.

Personal laptops are not allowed to be connected to the school network (other than via the School's VPN) without the permission of the Head of IT Services. The School has a set of laptops and Chromebooks which staff may arrange to borrow through the Head of IT Services.

Pupils

Pupils in the Summer term of Year 6 who commute to School independently are allowed to bring a mobile phone with them. Student phones should not be a smart phone or have internet connectivity. These must be handed in to the Form teacher at the start of the day and collected from Reception as they leave school. Pupils are not allowed to bring in any other devices that communicate over the internet including smartwatches and other wearable technology.

School mobile technologies available for pupil use including laptops, tablets, cameras, etc. are stored in the IT office. Access is available via Head of IT Services.

The school recognises that mobile devices are sometimes used by pupils for medical purposes or as an adjustment to assist pupils who have disabilities or special educational needs. Where a pupil needs to use a mobile device for such purposes, the pupil's parents should arrange a meeting with the pupil's Head of Section to agree how the school can appropriately support such use. The Head of Section will then inform the pupil's teachers and other relevant members of staff about how the pupil will use the device at school.

Use of internet and email

Staff

Staff must not access any website or personal email which is unconnected with school work or business from school devices or whilst teaching. Such access may only be made from staff members' own devices whilst away from the presence of pupils.

When accessed from staff members' own devices / off school premises, staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the school.

The school has taken all reasonable steps to ensure that the school network is safe and secure. Staff should be aware that email communications through the school network and staff email addresses are monitored.

Staff must immediately report to the Head or in his absence, the Deputy Head Pastoral and Operations, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to the Head of IT Services.

Any online communications must not either knowingly or recklessly:

- place a child or young person at risk of harm, or cause actual harm;
- bring Hurlingham into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
    - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
    - using social media to bully another individual; or
    - posting links to or endorsing material which is discriminatory or offensive.

Under no circumstances should school pupils, parents or former pupils under the age of 18 be added as social network 'friends' or contacted through social media.

Any digital communication between staff and pupils or parents must be professional in tone and content. Under no circumstances may staff contact a pupil or parent using any personal email address. The school

ensures that staff have access to their work email address when offsite, for use as necessary on school business.

Email protocols:

- the sending/forwarding of chain emails is not permitted;
- attachments from unrecognised senders or that look suspicious should not be opened;
- spam email received should be reported by pressing the 'report spam' button;
- the sending of bulk emails is acceptable only for a good reason associated with School;
- all externally addressed group emails should be addressed to admin@hurlinghamschool.co.uk and the individual recipients' email addresses entered in the BCC field.

Pupils

There is strong anti-virus and firewall protection on our network.

Pupils must not respond to any website or other communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication to; their class teacher, computing teacher or any other member of staff.

The school expects pupils to think carefully before they post any information online, or repost or endorse content created by other people. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others.

Pupils must report any accidental access to materials of an inappropriate nature directly to their class teacher, computing teacher or any other member of staff. Deliberate access to any inappropriate materials by a pupil will lead to the incident being reported to the Head and will be dealt with under the school's Behaviour, Rewards, Sanctions and Exclusion Policy. Pupils should be aware that all internet usage via the school's systems and its Wi-Fi network is monitored.

Certain websites are automatically blocked by the school's filtering system. If this causes problems for school work / research purposes, pupils should contact the Head of IT Services for assistance.

7. Managing online safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The Prep School DSL has overall responsibility for the school's approach to online safety, with support from deputies, the Head of Digital Strategy and Computing and the Head where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. Staff should consider how they tailor online safety provision to ensure vulnerable students receive information in an appropriate manner and can access the additional support they may need. If in doubt, staff should refer to the Teaching Online Safety in Schools (2023) UK government guidance.

The importance of online safety is integrated across all school operations in the following ways:

- Staff receive regular training
- Staff receive regular updates regarding online safety information and any changes to online safety guidance or legislation
- Online safety is integrated into learning throughout the curriculum

Handling online safety concerns

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Safeguarding and Child Protection Policy.

Concerns regarding a staff member's online behaviour are reported to the Head, who decides on the best course of action in line with the relevant policies, e.g. the Staff Code of Conduct, Allegations of Abuse Against Staff Policy, and Disciplinary Policy and Procedures. If the concern is about the Head, it is reported to the Principal.

Concerns regarding a pupil's online behaviour are reported to the Prep School DSL, who investigates concerns with relevant staff members, e.g. the Head and Head of IT Services, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour, Rewards, Sanctions and Exclusions Policy and the Safeguarding and Child Protection Policy.

Where there is a concern that illegal activity has taken place, the Head contacts the police.

The school avoids unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Safeguarding and Child Protection Policy.

All online safety incidents and the school's response are recorded by the Prep School DSL.

8. Cyberbullying

Cyberbullying can include the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Menacing or upsetting responses to someone in a chatroom
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy.

9. Child on child sexual abuse and harassment

All staff will be aware of the indicators of abuse, neglect and exploitation and understand where the risk of such harms can occur online. Staff will understand that this abuse can occur both in and outside of school and off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The school responds to all concerns regarding online child on child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child on child abuse are reported to the Prep School DSL, who will investigate the matter in line with the Child on child Abuse Policy and the Child Protection and Safeguarding Policy.

10. Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, including the following:

- The pupil believes they are talking to another child, when they are actually talking to an adult masquerading as someone younger with the intention of gaining their trust to abuse them.
- The pupil does not want to admit to talking to someone they met on the internet for fear of judgement, feeling embarrassed, or a lack of understanding from their peers or adults in their life.
- The pupil may have been manipulated into feeling a sense of dependency on their groomer due to the groomer's attempts to isolate them from friends and family.
- Talking to someone secretly over the internet may make the pupil feel 'special', particularly if the person they are talking to is older.
- The pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The Prep School DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.
- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the Prep School DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Prevent Duty Policy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Prevent Duty Policy.

11. Mental health

The internet, particularly social media, can be the root cause of a number of mental health issues in pupils, e.g. low self-esteem and suicidal ideation.

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health. Concerns about the mental health of a pupil will be dealt with in line with the Social, Emotional and Mental Health (SEMH) Policy.

12. Online hoaxes and harmful online challenges

For the purposes of this policy, an **"online hoax"** is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, **"harmful online challenges"** refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to the DSL immediately.

The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the Head will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing pupils.

- Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils.
- Proportional to the actual or perceived risk.
- Helpful to the pupils who are, or are perceived to be, at risk.
- Appropriate for the relevant pupils' age and developmental stage.
- Supportive.
- In line with the Child Protection and Safeguarding Policy.

Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, e.g. it encourages children to participate in age-inappropriate activities that could increase safeguarding risks or become a child protection concern, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or even to individual children at risk where appropriate.

The DSL and Head will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

13. Cyber-crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The school will factor into its approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a pupil's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

The DSL and Head will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully, and will ensure that pupils cannot access sites or areas of the internet that may encourage them to stray from lawful use of technology, e.g. the 'dark web', on school-owned devices or on school networks through the use of appropriate firewalls.

14. Use of technology in the Classroom

A wide range of technology is used during lessons, including the following:

- Computers
- Laptops & Chromebooks
- Tablets
- Intranet, including cloud-based storage services, such as Google Workspace or Microsoft365
- Email
- Cameras

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher always reviews and evaluates the resource. Class teachers ensure that any internet-derived materials are used in line with copyright law.

Pupils are supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

15. Use of smart technology

While the school recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which the school will ensure it manages.

Pupils will be educated on the acceptable and appropriate use of personal devices and will use technology in line with the school's Safe and Sensible Computing agreement.

Staff will use all smart technology and personal technology in line with the school's Staff Acceptable Use Policy and Agreement.

The school recognises that pupils' unlimited and unrestricted access to the internet via mobile phone networks means that some pupils may use the internet in a way which breaches the school's acceptable use of ICT agreement for pupils.

Inappropriate use of smart technology may include:

- Using mobile and smart technology to sexually harass, bully, troll or intimidate peers.
- Sharing indecent images, both consensually and non-consensually.
- Viewing and sharing pornography and other harmful content.

Pupils are not be permitted to have in their possession any smart devices or any other personal technology whilst in School.

The school will hold assemblies, where appropriate, which address any specific concerns related to the misuse of smart technology and outline the importance of using smart technology in an appropriate manner.

The school will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.

The school will consider the 4C's (content, contact, conduct and commerce) when educating pupils about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

16. Internet Access

Pupils, staff and other members of the school community are only granted access to the school's internet network once they have read and signed the Acceptable Use Agreement. A record is kept of users who have been granted internet access by the Head of IT Services.

All members of the school community are encouraged to use the school's internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

17. Data storage and processing

The school takes its compliance with the Data Protection Act 2018 seriously. Please refer to the Data Protection Policy, the Staff Acceptable Use Policy and Agreement, the Mobile Devices Policy, the Taking, Storing and Using Images of Children Policy and the Social Media Policy for further details.

Staff and pupils are expected to save all data relating to their work to either a Google drive or the staff drive school's central server.

Staff devices should be encrypted if any data or passwords are stored on them. The school expects all removable media (USB memory sticks, CDs, portable drives) taken outside school or sent by post or courier to be encrypted by the Head of IT Services before sending. However, the use of these should be kept to an absolute minimum and remote access via the School's VPN should always be the primary method of storage.

Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or pupils should be stored on personal memory sticks.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be reported immediately to the Head or the E-Safety Officer.

Retention of digital data

Teaching staff must be aware that all emails sent or received on school systems will be routinely deleted after 2 years and email accounts will be closed and the contents within 6 months of that person leaving the school. Important information that is necessary to be kept should be held on the relevant personnel or pupil file, not kept in personal folders, archives or inboxes. Hence it is the responsibility of each account user to ensure that important information (or indeed any personal information that they wish to keep, in line with school policy on personal use) is retained in the right place or, where applicable, provided to the right colleague. That way no important information should ever be lost as a result of the school's email deletion protocol.

If a member of staff considers that reasons exist for the protocol not to apply or need assistance in how to retain and appropriately archive data, they should contact The Head of IT Services.

Breach reporting

The law requires the school to notify personal data breaches, if they are likely to cause harm, to the authorities and, in some cases, to those affected. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This will include almost any loss of, or compromise to, personal data held by the school regardless of whether the personal data falls into a third party's hands. This would include:

- loss of an unencrypted laptop, USB stick or a physical file containing personal data;
- any external hacking of the school's systems, eg through the use of malware;
- application of the wrong privacy settings to online systems;
- misdirected post, fax or email;
- failing to bcc recipients of a mass email; and
- unsecure disposal.

The school must generally report personal data breaches to the ICO without undue delay (ie within 72 hours), and certainly if it presents a risk to individuals. In addition, controllers must notify individuals affected if that risk is high. In any event, the school must keep a record of any personal data breaches, regardless of whether we need to notify the ICO.

If either staff or pupils become aware of a suspected breach they should contact the Principal in the case of staff and children should notify their teacher.

Data breaches will happen to all organisations, but the school must take steps to ensure they are as rare and limited as possible and that, when they do happen, the worst effects are contained and mitigated. This requires the involvement and support of all staff and pupils. The School's primary interest and responsibility is in protecting potential victims and having visibility of how effective its policies and training are. Accordingly, falling victim to a data breach, either by human error or malicious attack, will not always be the

result of a serious conduct issue or breach of policy; but failure to report a breach will be a disciplinary offence.

18. Password security and logging on and off

Staff have individual school network logins, email addresses and storage folders on the server. Staff are regularly reminded of the need for password security.

All staff members of staff should:

- use a strong password (usually containing eight characters or more, and containing upper and lower case letters as well as numbers), which should be changed every 90 days;
- not write passwords down;
- not share passwords with other pupils or staff;
- not attempt to gain unauthorised access to anyone else's computer or to confidential information to which you do not have access rights
- not log on as someone else nor use a computer which has been logged onto by someone else;
- log off when leaving a workstation, even for a short time, or lock the workstation if no other user is likely to need to use it.

19. Safe use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet.

Parents are welcome to take videos and digital images of their children at school events for their own personal use in line with the School's Mobile Devices Policy. To respect everyone's privacy and in some cases protection, these images should not be published on blogs or social networking sites (etc.) without the permission of the parents of children identifiable in them (or in the case of adults the permission of the individuals themselves). The most senior members of staff present at any play or performance reminds parents of this requirement.

Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow this policy and the Staff Acceptable Use Policy and Agreement , the Mobile Devices Policy, the Taking, Storing and Using Images of Children Policy and the Social Media Policy concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment: personal equipment should not be used for such purposes.

Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Written permission from parents will be obtained before photographs of pupils are published on the school website (see the School's Parent Contract and Acceptable Use Policy for more information) or on any of the School's social media accounts.

Photographs published on the school website, social media accounts or displayed elsewhere, that include pupils, will be selected carefully and will comply with good practice guidance on the use of such images. Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs. See the School's Social Media Policy for more detail.

20. Misuse

Illegal Activity

Hurlingham School will not tolerate illegal activities or activities that are inappropriate in a school context and will, depending on the nature of the concern or allegation, report illegal activity to the police, the LSCB, DBS, LADO or other external agency as appropriate. If the school discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the CEOP. Incidents of misuse or suspected misuse will be dealt with in accordance with the School's policies and procedures (in particular the Safeguarding and Child Protection Policy).

If anyone suspects that access has been attempted to any website or inappropriate material of any type is found on any electronic device then they must report all concerns, allegations, complaints or suspicions to the DSL, Head or E-Safety officer unless that person is the subject of the concern.

If anyone has concerns about other forms of illegal IT activity such as copyright theft, fraud or the use of unlicensed software, this must be reported to the E-Safety Officer who will inform the Head and the Head of IT Services for investigation.

In the event that a member of staff who has raised a concern feels that it is not being addressed then they should follow the School's whistleblowing procedure detailed in the Staff Handbook.

Inappropriate Activity

It is expected that all members of the School Community will behave responsibly and adhere to all of the School's policies and procedures. However, careless, irresponsible or deliberate misuse of IT equipment of services should be reported in the following ways.

- E-safety incidents which do not raise safeguarding concerns or illegal activity should be reported to the E-Safety Officer.
- Misuse of IT equipment or services by staff, visitors or pupils should be reported to the E-Safety Officer.
- Misuse detected by the Head of IT Services should be reported to the E-Safety Officer.

Any suspected Data breaches must be reported to the Data Protection Officer.

Investigating Incidents

Depending on the nature of the incident, the E-Safety Officer, Head or DSL will instruct the Head of IT Services to investigate in the following way:

- examine all technical logs;
- examine the firewall and filter systems;
- remote examination of the School's desktops and laptops connected to the School network;
- examine relevant School emails, (including sent and deleted).

There should be two senior members of staff involved in this process, ideally the Head of IT Services should do this in conjunction with the E-Safety Officer and (depending on the nature of the concern) the DSL.

A record of the URL of any site containing the alleged misuse will be made describing the nature of the content causing concern and unsuitable materials will be copied. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed

and attached to the report (except in the case of images of child sexual abuse or any other indecent images of children– see below)

Following the investigation the Head of IT Services and the Head of E-Safety will report their findings to the DSL, the Principal and Head. If it is considered that there is cause for concern then appropriate action will be required and could include the following:

Internal response or discipline procedures in accordance with the School's Behaviour and Anti-bullying Policies;

- Contacting the Local Authority or any other appropriate agencies;
- Reporting the incident to the Police;
- If the security of personal data has been compromised, consideration of whether a report to the Information Commissioner's Office is appropriate.

If content being reviewed includes images of child abuse then the monitoring will be halted, the DSL, the Head and the Principal will be informed and the computer will be confiscated and held securely. The matter will then be referred to the Police immediately.

Other instances to report to the police would include:

- incidents of 'grooming' behaviour;
- the sending of obscene materials to a child, including those produced by children (sexting);
- adult material which potentially breaches the Obscene Publications Act;
- criminally racist material;
- other criminal conduct, activity or materials.

Incidents of misuse by members of staff will be dealt with through disciplinary procedures set out in the Disciplinary Policy and Procedure.

Incidents of misuse by pupils will be dealt with through disciplinary procedures set out in the School's Behaviour and Anti-bullying Policies. The school will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our Anti-Bullying Policy.

21. Monitoring and Managing Access and Security

Staff, parents and pupils should be aware that school email and internet usage (including through school Wi-Fi) will be monitored for safeguarding, conduct and performance purposes, and both web history and school email accounts may be accessed by the school where necessary for a lawful purpose – including serious conduct or welfare concerns, extremism and the protection of others.

Any personal devices used by pupils, whether or not such use is permitted, may be confiscated and examined under such circumstances. The school may require staff to conduct searches of their personal accounts or devices if they were used for school business in contravention of this policy.

The school will provide managed internet access to its staff and pupils in order to help pupils to learn how to assess and manage risk, to gain the knowledge and understanding to keep themselves safe when using the internet and to bridge the gap between school IT systems and the more open systems outside school.

- The school will use a recognised internet service, currently Vaioni.
- The school will ensure that all internet access has age appropriate filtering provided by a recognised filtering system which is regularly checked to ensure that it is working, effective and reasonable, currently through Senso.cloud.
- The school will ensure that its networks have virus and anti-spam protection, currently ESET Endpoint.
- Access to school networks will be controlled by personal passwords.
- Systems will be in place to ensure that internet use can be monitored and a log of any incidents will be kept to help to identify patterns of behaviour and to inform e-safety policy.

- The security of school ICT systems will be reviewed regularly by the Head of IT Services in conjunction with the E-Safety Officer.
- The school will ensure that access to the internet via school equipment for anyone not employed by the school is similarly filtered and monitored.

22. Educating Parents

The school works in partnership with parents to ensure pupils stay safe online at school and at home. Parents are provided with information about the school's approach to online safety and their role in protecting their children. Parents are sent a copy of the Safe and Sensible Computing agreement at the beginning of each academic year and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

Parents will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- Sharing of indecent imagery of pupils, e.g. sexting.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

Parental awareness regarding how they can support their children to be safe online is raised in the following ways:

- Parents' evenings
- Twilight training sessions
- Newsletters
- Regular updates and resources from National Online Safety

23. Complaints

As with all issues of safety at Hurlingham School, if a member of staff, a pupil or a parent has a complaint or concern relating to e-safety prompt action will be taken to deal with it. Complaints should be addressed to the appropriate Head of Section who will ask the Head of E-Safety to undertake an investigation where appropriate. Please see the Complaints Policy for further information. Any complaints received must be recorded as an incident on the School's CPOMS platform.

Incidents of or concerns around e-safety will be recorded using the incident reporting system on the School's CPOMS platform and this will include a notification to the Head of E-Safety, The Head, The Principal and the DSL, in accordance with the School's Child Protection Policy.