



Online Safety Policy

Policy date:	March 2026
Date of next review:	March 2027
Owner:	Deputy Head (Pastoral)/ DSL
Leadership Team:	Online Safety Committee/ Senior Leadership Team
Intended audience:	Pupils, Parents, Staff and Visitors
Location:	School Portal

1. Introduction

- 1.1 It is the duty of Haileybury to ensure that every pupil in its care is safe; and the same principles apply to the digital world as apply to the real world. Online communications and technology provide opportunities for enhanced learning, but also pose great 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 bullying, harassment, grooming, stalking, abuse and radicalisation and identity theft.
- 1.2 Technology is continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. However, many information technologies, particularly online resources, are not effectively policed. All users need to be aware, in an age-appropriate way, of the range of risks associated with the use of these internet technologies. Current and emerging technologies used in and outside of School include:
- Websites;
 - Email and instant messaging;
 - Blogs, forums and chat rooms;
 - Mobile internet devices such as smart phones and tablets;
 - Social networking sites;
 - Music / video downloads;
 - Gaming sites and online communities formed via games consoles;
 - Instant messaging technology via SMS or social media sites;
 - Video calls;
 - Podcasting and mobile applications;
 - Virtual and augmented reality technology; and
 - Artificial intelligence.
- 1.3 Technology is a vital part of education and modern life, but its use also presents significant safeguarding challenges, including:
- **Content:** exposure to harmful or inappropriate material.
 - **Contact:** risks of grooming, exploitation, or harmful online relationships.
 - **Conduct:** risks from pupils' own behaviour, such as bullying, sexting, or sharing personal information.
 - **Commerce:** risks from fraud, scams, or exposure to advertising and manipulative content.
- These "4Cs" risks are recognised in statutory guidance and underpin Haileybury's approach to online safety.
- 1.4 Haileybury is committed to ensuring that all members of the School community can benefit from the opportunities that digital technologies provide while remaining safe from harm. Online safety is integral to safeguarding and permeates all aspects of School life.
- 1.5 Haileybury understands the responsibility to educate pupils on online 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. The School also understands the importance of involving pupils in discussions about online safety and listening to their fears and anxieties as well as their thoughts and ideas.

2. Aims

- 2.1 This policy 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 linked to the following School policies:
- Safeguarding and Child Protection Policy
 - ICT Acceptable Use Policy

- Rewards, Behaviour and Sanctions Policy
- Mobile Phone and Electronic Device Policy
- Artificial Intelligence (AI) Policy
- Countering Bullying Policy
- Data Protection Policy (and Privacy Notices)
- Social Media Policy
- Taking, Storing and Using Images of Children Policy

2.2 These collectively form the School's online safety framework.

3. Scope

- 3.1 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.
- 3.2 This policy, and others referred to above, cover both fixed and mobile internet devices provided by the School (such as PCs, laptops, webcams, tablets, whiteboards, 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.).
- 3.3 In designing this policy, the School has considered the "4Cs" outlined in KCSIE (content, contact, conduct and commerce) and detailed above, as the key areas of risk. However, the School recognises that many pupils will have unlimited and unrestricted access to the internet via mobile phone networks. This means that some pupils, may use mobile technology to facilitate child-on-child abuse, access inappropriate or harmful content or otherwise misuse mobile technology whilst at School. The improper use of mobile technology by pupils, in or out of School, will be dealt with under the School's Rewards, Behaviour and Sanctions Policy and / or Safeguarding and Child Protection Policy as is appropriate in the circumstances.

4. Roles and responsibilities in relation to online safety

- 4.1 All staff, governors and visitors have responsibilities under the safeguarding policy to protect children from abuse and make appropriate referrals. The following roles and responsibilities must be read in line with the Safeguarding and Child Protection Policy.
- 4.2 Governing Body: The Governing Body has overall leadership responsibility for safeguarding as outlined in the Safeguarding and Child Protection Policy, and has oversight of online safety arrangements.
- 4.3 The Master and the Executive Leadership Team (ELT): The ELT is responsible for the safety of the members of the School community and this includes responsibility for online safety. They are responsible for procuring appropriate filtering and monitoring systems, documenting decisions on what is blocked or allowed and why, reviewing the effectiveness of the filtering and monitoring provisions, overseeing reports and ensuring staff are appropriately trained.
- 4.4 Designated Safeguarding Lead (DSL): As set out in the Safeguarding and Child Protection Policy, the DSL takes the lead responsibility for online safety at Haileybury and also has the role of Online Safety Coordinator (see below).
- 4.5 The DSL will ensure that this policy is upheld at all times. As such, in line with the Safeguarding and Child Protection policy, the DSL will take appropriate action if in receipt of a report that engages that policy relating to activity that has taken place online.
- 4.6 Online Safety Coordinator: Responsible for day to day management of online safety. They will keep up to date on current online safety issues and guidance issued by relevant organisations,

including the Department for Education (including KCSIE), ISI, the CEOP (Child Exploitation and Online Protection), Childnet International and the Local Safeguarding Children Procedures.

- 4.7 The Online Safety Coordinator works closely with the Online Safety Group consisting of the DSL, the Deputy Head (Pastoral) Assistant Head (Pastoral), the Director of Digital Innovation and Enterprise, the Director of Technology, Information and Data Systems, and the Assistant Head (Pupil Progress and Behaviour). This group meets half termly and takes responsibility for issues regarding online safety, filtering and the monitoring systems and usage.
- 4.8 Director of Technology, Information and Data Systems: Along with the School's IT Department, the Director of Technology, Information and Data Systems has a key role in maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments. They are responsible for 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. Responsible for ensuring that the School has in place a robust filtering and monitoring system, and ensuring that it is reviewed and tested regularly to ensure effectiveness. They monitor the use of the internet and emails, maintain content filters, and will report inappropriate usage to the Online Safety Coordinator/ DSL.
- 4.9 Director of Digital Innovation and Enterprise: Responsible for ensuring the appropriate use of AI technologies (see the AI Policy).
- 4.10 Staff: All staff must model safe online behaviour, comply with the ICT Acceptable Use Policy, and report concerns. Staff must also enforce this policy in accordance with direction from the DSL, the Master and other senior leaders as appropriate.
- 4.11 Pupils: Expected to behave responsibly online and comply with the ICT Acceptable Use Policy as well as other relevant policies including the Rewards, Behaviour and Sanctions Policy, Mobile Phone and Electronic Device Policy, and AI policies.
- 4.12 Parents: It is essential for parents to be fully involved with promoting online safety both within and outside school. The School regularly consults and discusses online safety with parents and seeks to promote a wide understanding of the benefits and risks related to internet usage. The School will 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.

5. Education and Training

- 5.1 **Pupils:** The school provides opportunities to teach about online safety within a range of curriculum areas such as wellbeing, computer science (LS), digital innovations (Removes) lessons and via talks, presentations and assemblies.. Educating pupils on the dangers of technologies that may be encountered outside school will also be carried out informally when opportunities arise.
- 5.2 At age-appropriate levels, pupils are taught about their online safety responsibilities and to look after their own online safety.
- 5.3 Pupils can report concerns to the Online Safety Coordinator/DSL and any member of staff at the school.
- 5.4 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 Safeguarding and Child Protection, Countering Bullying, and Rewards, Behaviour and Sanctions Policies, which describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying).

- 5.5 Pupils should approach the DSL, or any other member of staff they trust, as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.
- 5.6 **Staff:** As part of their induction, all staff receive safeguarding training that includes online safety, with annual updates and additional AI literacy training.
- 5.7 All staff receive regular information and training on online safety issues via formal training (at INSET days) and internal meeting time, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety.
- 5.8 All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following the school's Online Safety procedures.
- 5.9 **Parents:** The School seeks to work closely with parents and guardians in promoting a culture of online safety. Parents are supported through guidance and, where appropriate, information sessions to help them reinforce online safety at home.
- 5.10 The school will 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.

6. Filtering, Monitoring and Security

- 6.1 Haileybury aims to provide a safe environment to learn and work, including when online. Filtering and monitoring are important parts of the school's safeguarding arrangements and it is vital that all staff understand the expectations, applicable roles and responsibilities in relation to filtering and monitoring.
- 6.2 The School uses filtering and monitoring systems to identify, and reduce exposure to, harmful content.
- 6.3 The Director of Digital Innovation and Enterprise, alongside the Director of IT team, ensures these systems remain effective.
- 6.4 New technologies, including AI systems, undergo a Data Protection Impact Assessment (see AI Policy).
- 6.5 Serious incidents are dealt with under the Safeguarding and Child Protection policy.

7. The use of technology and behaviour

- 7.1 Pupils are required to follow the ICT Acceptable Use Policy which sets expectations for internet, device, and system use, and the Mobile Phone and Electronic Device Policy which sets out clear guidelines for when devices may or may not be used.
- 7.2 Misuse of devices is addressed under the Rewards, Behaviour and Sanctions Policy, which includes sanctions for digital misconduct (e.g. cyberbullying, sexting, or iPad misuse) and the Mobile Phone and Electronic Device Policy.
- 7.3 The AI Policy governs safe and ethical use of generative AI, bans deep fakes, and prohibits AI-enabled wearables.

8. Online communications and use of social media

- 8.1 The expectations for staff use of social media is set out in the Social Media Policy.

- 8.2 **Pupils:** The School expects pupils to think carefully before they post any information online, or repost or endorse content created by other people. Content posted must not be, or potentially be, inappropriate or offensive, or likely to cause embarrassment to an individual or others or bring the school into disrepute. The School takes misuse of technology by pupils very seriously and incidents will be dealt with under the Rewards, Behaviour, and Sanctions Policy, the Safeguarding and Child Protection Policy and the Countering Bullying Policy as appropriate.

9. Safe use of digital and video images

- 9.1 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 / carers 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.
- 9.2 Pupils will be educated 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 (personal) images on the internet (e.g. on social networking sites).
- 9.3 The Taking, Storing and Using Images of Children Policy provides guidance to staff and information to pupils and their parents, carers or guardians about how images of pupils are normally used by Haileybury. It also covers the School's approach to the use of cameras, video and filming equipment at school events and on school premises by parents and pupils themselves, and the media.

10. Data Protection

- 10.1 Please refer to the Data Protection policy for further details as to the key responsibilities and obligations that arise when personal information, particularly that of children, is being processed by or on behalf of the school.
- 10.2 Staff and pupils must not share personal data online without authorisation (see ICT Acceptable Use Policy).
- 10.3 AI use is subject to safeguards to prevent sharing of personal or sensitive information (see AI Policy).
- 10.4 Data Protection Impact Assessments are completed for all new digital tools.

11. Reporting and responding to Concerns

- 11.1 If a member of staff discovers that a child or young person is at risk as a consequence of online activity they must report their concerns to the DSL or Deputy DSLs, and where appropriate, record this on CPOMS. Safeguarding concerns take precedence and are escalated according to the Safeguarding and Child Protection Policy.
- 11.2 Staff and pupils are required to report any misuse or breaches.
- 11.3 The School will not tolerate illegal activities or activities that are in breach of the policies referred to above. Where appropriate the school will report illegal activity to the police and/or the local safeguarding partnerships.
- 11.4 Sanctions will follow the Rewards, Behaviour and Sanctions Policy, ICT Acceptable Use Policy, or Mobile Phone and Electronic Device Policy, depending on the nature of the incident.

Version history		
Date	Reviewed by	Notes
October 2025	Deputy Head (Pastoral) and Director of Digital Innovation and Enterprise	New policy drafted.
March 2026	Online and IT Committee	Reviewed
March 2026	Senior Leadership Team	Reviewed
March 2026	Executive Leadership Team	Reviewed and approved