Hartismere School

Online/AI Policy

Policy No 24

Led By: EJW Reviewed: February 2026 Next review: February 2027

Purpose

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school digital technology systems, both in and out of the school.

This policy describes our approaches to the filtering and monitoring of online activity, and bridges our school's behaviour, safeguarding and child protection policies where there is an online element. This should be read in conjunction with those policies, and other relevant policies.

Roles and Responsibilities

At Hartismere School the Headteachers are responsible for identifying a senior member of staff to be the **Designated Online Safety Lead** (Mr E Waller). Through appropriate training, knowledge and experience our Designated Online Safety Lead will establish and review our online safety policies and documents.

The Designated Online Safety Lead will lead our **Online Safety Group** and work with the **Designated Safeguarding Lead** to promote awareness of online safety across the school community, liaise with appropriate curriculum leaders to ensure online safety curriculum coverage, ensure staff are aware of procedures relating to online safety incidents and use reports of incidents to inform future online safety developments.

The Designated Online Safety Lead will work with our school **Network Manager** or **Managed Service Provider** to ensure the integrity and robustness of our school's equipment, network and internet access.

Online Safety

The internet presents many opportunities for development, however the risks and challenges must be mitigated to ensure the school community is as safe as possible.

There are a breadth of online issues that are ever-evolving, but our approach to online safety is governed by helping to protect our students from the dangers outlined by the 4Cs:

- Content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

- Contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- Conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying), and
- Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

Internet Access, Filter and Firewall

Our school uses a robust multi-layered firewall, filtering and monitoring solution (Smoothwall) for all incoming and outgoing internet traffic. The filtering helps to ensure that the content of web traffic is appropriate for students and that, where possible, commerce websites are restricted.

The nature of the internet means that not all inappropriate content can be foreseen, which is why the designated Online Safety Lead is able to amend the internet filter block-lists and whitelists in response to concerns from staff and students.

All users are identified and authenticated on the system and differentiated filters are applied for our staff, high school students, sixth formers and visitors. All filters include the categories on the Internet Watch Foundation CAIC list.

We use active monitoring to alert designated staff of every attempt made by our users to access filtered websites including those pertaining to terrorism, extremism and pornography. This allows for the conduct of the user to be logged with appropriate action taken upon investigation.

Curriculum

Embedding online safety into the curriculum, in particular RSHE, the pastoral programme and computer science, allows for the modelling of online behaviour, the content risks and the dangers of making contact with others online to be taught.

Artificial Intelligence (AI)

Hartismere recognises that generative AI is a rapidly evolving field, necessitating a dynamic approach to maintain our legal and ethical responsibilities as identified by the **DfE, JCQ** and the **Online Safety Act**.

These responsibilities include the protection of **Intellectual Property Law**, **Data Protection**, and the statutory requirements of **Keeping Children Safe in Education**.

As AI capabilities change in real time, staff and students must remain vigilant against emerging risks, including **misinformation** and the exposure to **illegal or inappropriate content**.

To safeguard the school community, users must critically verify all AI-generated outputs and are strictly prohibited from inputting sensitive data or personally identifiable information into these systems.

In line with our commitment to **filtering and monitoring**, the school will regularly review AI usage to ensure it adheres to our safeguarding standards and ethical expectations regarding **plagiarism** and academic integrity.

Mobile Technologies

“Bring Your Own Device” (BYOD)

Pupils are not allowed to have mobile phones or smart wear, including, but not exclusive, to smart watches or smart glasses, in school.

Students in the sixth form are permitted to have their mobile phones in school. They are not permitted to use, or have them out in lessons unless given explicit permission by the teacher. They are expected to use their mobile phones responsibly and adhere to the school's code of conduct.

Our school has a WiFi network for staff, sixth formers and visitors that is on a separate VLAN from our main network. Internet access on our WiFi network is subject to the same filtering and monitoring above.

We appreciate that our staff want to access their school email accounts on their own device and when they're at home. We have enforced two step authentication on our email and cloud computing accounts for staff as an additional layer of security.

Procedures

Our pupils are responsible for using the school's digital technology systems in accordance with our *Home/School Agreement about student use of school computer equipment and access to the internet*. Our behaviour policies include procedures and sanctions supporting this.

All student activity on school computer equipment is recorded.

Our staff are made aware of their roles and responsibilities to ensure online safety. This includes monitoring the internet activity of children they teach in a computer room, and responding to any report of peer-on-peer abuse or misconduct in accordance with our safeguarding and behaviour policies.

Incidents of online peer-on-peer abuse, online harassment, indecent image sharing, or other safeguarding matters with an online element will be reported in accordance with our Safeguarding Policies and our Designated Online Safety Lead will provide technical expertise to our Designated Safeguarding Lead.