

Online Safety Policy

Reviewer: Deputy Head of College / Deputy Head (Pastoral)

Approved by SMT: August 2026

1. Purpose

Hurstpierpoint College recognises that technology plays a vital role in education, communication and daily life. The College seeks to provide pupils with the knowledge, skills and resilience to utilise digital technologies safely, responsibly and effectively.

The College is committed to safeguarding and promoting the welfare of children and expects all members of the College community to share this commitment. Online safety is viewed as a safeguarding issue and forms an integral part of the College's wider safeguarding arrangements.

This policy should be read in conjunction with:

- Safeguarding and Child Protection Policy
- Behaviour Policy
- Use of Artificial Intelligence (AI) Policy
- IT Policy (Acceptable Use Agreements)
- Data Protection Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Pupil Use of Mobile Phones Policy

The aims of this policy are:

- To safeguard pupils when using digital technology.
- To promote safe, responsible and respectful use of online services.
- To develop pupils' digital literacy and critical thinking skills.
- To ensure that staff understand their responsibilities regarding online safety.
- To minimise the risk of exposure to harmful, inappropriate or illegal content.
- To reduce the risk of cyberbullying and online abuse.
- To ensure compliance with statutory safeguarding obligations, including Keeping Children Safe in Education (KCSIE).

The College recognises that technologies and online risks evolve rapidly. This policy will be reviewed regularly and updated as required.

2. Online Risks

The College recognises that online risks can be broadly categorised as:

Content

Exposure to harmful, misleading, inappropriate or illegal content.

- Examples include:
 - extremist content
 - hate content
 - misinformation and disinformation
 - pornography

- self-harm material
- gambling-related material

Contact

Online interactions that place a child at risk.

- Examples include:
 - grooming
 - exploitation
 - coercion
 - radicalisation
 - online harassment

Conduct

Behaviour by users which causes harm.

- Examples include:
 - cyberbullying
 - sharing inappropriate images
 - online abuse
 - impersonation
 - misuse of AI technologies

Commerce

Risks involving online financial activity.

- Examples include:
 - scams
 - phishing
 - fraud
 - inappropriate purchases
 - exploitation through gaming or social media platforms

3. Responsibilities

Governors have oversight of safeguarding arrangements, including online safety, and receive appropriate reports regarding safeguarding risks and trends. Governors will satisfy themselves that appropriate filtering and monitoring systems are in place, regularly reviewed and effective in safeguarding pupils.

The Head of College has overall responsibility for ensuring that appropriate online safety procedures are implemented throughout the College.

The DSL leads on online safety safeguarding concerns, oversees staff training, monitors emerging online risks and liaises with external agencies where necessary.

All **staff** are responsible for:

- promoting safe online behaviours;
- modelling appropriate technology use;
- reporting online safety concerns promptly;
- following acceptable use procedures;
- maintaining professional boundaries online.

Pupils are expected to:

- use technology responsibly;
- respect the rights of others online;
- report concerns promptly;
- comply with College expectations regarding technology use.

Parents

The College encourages parents to:

- engage with their child's online activity;
- promote safe technology use at home;
- notify the College of significant online safety concerns where appropriate.
- encourage responsible online behaviour and awareness of digital footprints.

Curriculum

Online safety education is embedded in the PSHCE curriculum, the Tutorial programme and the academic curriculum more broadly. Topics include:

- privacy and personal information;
- passwords and account security;
- social media;
- digital footprints;
- cyberbullying;
- fake news and misinformation;
- consent and image sharing;
- online gaming
- understanding AI Chatbots
- making good choices online
- online scams and sextortion
- sharing nudes
- online blackmail
- deepfakes
- risks of Ai and misinformation
- managing risk online
- developing online safety skills
- healthy use of technology;
- online relationships;
- online reputation;
- the safe use of Artificial Intelligence.

Online safety education is delivered through:

- PSHCE
- Assemblies
- Tutor periods
- Visiting speakers
- The broader academic curriculum

Cyberbullying

Cyberbullying is treated as seriously as any other form of bullying.

- Examples include:
- abusive messaging;
- exclusion from online groups;
- sharing harmful content;

- posting offensive comments;
- impersonation.
- Incidents will be investigated in accordance with the Behaviour and Anti-Bullying Policies.
- Where necessary, sanctions may be imposed even where behaviour occurs away from the College site.

Use of College Systems

Users must:

- Only access systems using their own credentials;
- keep passwords secure;
- log out when devices are unattended;
- use technology for legitimate educational purposes;
- comply with copyright requirements;
- comply with the Acceptable Use Agreement.

Users must not:

- attempt to bypass filtering systems;
- access inappropriate material;
- use another person's account;
- install unauthorised software;
- engage in illegal activity;
- intentionally disrupt College systems.
- The College reserves the right to monitor and investigate the use of College systems where appropriate for any user.

Social Media

Staff and pupils should be aware that:

- material published online may remain accessible indefinitely;
- online activity can have safeguarding and reputational consequences;
- interactions between staff and pupils on personal social media platforms are inappropriate.
- staff must comply with the Staff Code of Conduct regarding social media use.
- pupils are expected to use social media respectfully and responsibly.
- for all users it is his strongly recommended to keep social media profiles on private and to not post identifying content e.g. school, address, full name, DOB.

Artificial Intelligence

The use of Artificial Intelligence must comply with the College's Use of Artificial Intelligence Policy.

- Users must:
- critically evaluate AI-generated content;
- acknowledge AI use where required;
- avoid submitting AI-generated work as their own;
- avoid entering confidential or personal information into public AI systems.

4. Filtering and Monitoring

The College implements appropriate and effective filtering and monitoring systems in accordance with statutory safeguarding guidance. These systems are regularly reviewed to ensure that they remain suitable for the age of pupils, the technologies used and emerging safeguarding risks.

Where monitoring identifies a safeguarding concern, the matter will be referred to the Designated

Safeguarding Lead. Incident logging, about pupils, and follow up actions to reduce the risk of harm will be recorded on CPOMS.

5. Mobile Devices

The use of mobile devices must comply with College rules applicable to each section of the College, as set out in the Pupil Use of Mobile Phones Policy.

Pupils must not:

- photograph or record others without consent;
- distribute images without permission;
- use devices in a manner which compromises safeguarding, privacy or dignity.
- Any misuse may result in disciplinary sanctions.

Staff:

- should not take pictures or videos of pupils on personal devices. If this is not possible, any media must be uploaded to school systems and to deleted off the personal device as soon as possible.
- use personal phones discreetly
- must not share personal details with pupils
- all staff working in the EYFS area must adhere to the EYFS Mobile Devices Policy.

6. Online Safety Incidents

Any concerns relating to any of the following must be reported immediately to a member of staff and passed on to the Safeguarding Team. Safeguarding concerns arising online will be managed in accordance with the College Safeguarding and Child Protection Policy. Incidents of online safety will be reported on CPOMS, using the relevant category.

- inappropriate content;
- cyberbullying;
- online exploitation;
- generating or sending nude or semi-nude images / youth-produced sexual imagery;
- harmful AI misuse;
- grooming;
- radicalisation;
- online sexual harassment;
- online sexual abuse;
- coercive or controlling behaviour facilitated through technology.

7. Staff Training

All staff receive regular safeguarding training which includes online safety.