



Document Control
Reference: Online Safety Policy
Version No: 1
Version Date: September 2026
Review Date: September 2027



**THE
HAYLING
COLLEGE**

Happy, Healthy, High Performing

Online Safety Policy

Date of Policy: September 2026
Date approved by Gobs: September 2026
Date of Next Review: September 2027

1. Aims and principles

The Hayling College will provide a safe digital environment in which pupils can learn, communicate and develop the knowledge and resilience to use technology safely. Online safety is a safeguarding responsibility and a running, interrelated theme across child protection, curriculum, behaviour, SEND, staff conduct, data protection and ICT management.

- Protect and educate pupils, staff, governors, volunteers and visitors in their use of technology.
- Identify pupils and groups who may be at greater risk online and make reasonable, proportionate adjustments.
- Maintain clear systems to identify, record, intervene in and escalate online-safety concerns.
- Use technology to support teaching and learning without exposing pupils or the school to avoidable safeguarding, privacy or cyber-security risk.

2. The four areas of online risk

Content: Illegal, inappropriate or harmful material, including pornography, racism, misogyny/misandry, self-harm, suicide, antisemitism, radicalisation, extremism, extreme violence, misinformation, disinformation, conspiracy theories and harmful AI-generated content.

Contact: Harmful interaction with other users or systems, including peer pressure, grooming, exploitation, harmful advertising and generative AI applications that simulate human interaction or intimacy.

Conduct: Behaviour that causes or increases harm, including bullying, harassment, sexual harassment, abusive messaging, nudes/semi-nudes, AI-generated sexual imagery, deepfakes, impersonation and unsafe sharing.

Commerce: Gambling, scams, phishing, financial exploitation and inappropriate advertising.

3. Roles and governance

3.1 Governing Body

- Has overall strategic responsibility for online safety and appropriate filtering and monitoring.
- The Safeguarding Governor, Erika Anders, oversees online safety and filtering/monitoring on behalf of FGB and provides challenge and assurance.
- Will receive assurance that filtering and monitoring are effective, reviewed at least annually, and actions completed.
- Will ensure staff training includes online safety and filtering/monitoring responsibilities.
- Will ensure online-safety teaching is adapted for vulnerable pupils and pupils with SEND where needed.

3.2 Headteacher and senior leadership

- Implement this policy consistently and resource it appropriately.
- Assign a responsible SLT lead for digital technology/filtering and monitoring and ensure clear cover and escalation.
- Approve and document temporary exceptions to filtering/monitoring; the DSL assesses safeguarding implications.
- Risk assess new technologies, including AI, before deployment where safeguarding, privacy or security risk may arise.

3.3 Designated Safeguarding Lead (DSL) - Helen Cox, Assistant Headteacher (AHT), SLT

- Leads online safeguarding and works with the Headteacher, DSL (Assistant Headteacher / SLT) and IT support.
- Understands filtering and monitoring and reviews relevant alerts/reports, including SENSO outputs.
- Responds to safeguarding concerns identified through monitoring and records safeguarding decisions/actions on CPOMS.
- Provides governors with assurance on effectiveness, trends, incidents, training and review actions.

3.4 IT support / ICT manager

- Maintains filtering, monitoring, device and network controls and provides understandable reports.
- Checks systems on school-managed devices and new devices/services before use.
- Escalates safeguarding concerns to the DSL and records technical checks, changes, failures and corrective action.

3.5 All staff, volunteers and contractors

- Maintain “it could happen here” online as well as offline.
- Supervise pupils using devices and report safeguarding concerns to DSL/DDSL without delay.
- Know how to report filtering/monitoring failures, over-blocking or unsafe content and never bypass controls without approval.
- Do not view, copy, print, save, forward or ask a pupil to share suspected indecent imagery; refer immediately to the DSL in line with safeguarding procedures.
- Use school systems and AI in accordance with Acceptable Use, Staff Code of Conduct and data-protection requirements.

4. Filtering and monitoring

The College uses technical filtering and monitoring, including SENSO monitoring of pupil activity. Technical controls do not replace active staff supervision.

- High-risk alerts will receive prompt safeguarding review; weekly SENSO reports will be reviewed for incidents and trends.
- Provision will be reviewed at least once each academic year and after significant risk, major technology/configuration change, new AI deployment or material failure.
- The review will involve SLT, DSL, IT support and the Safeguarding Governor (Erika Anders) and consider pupil risk profile including SEND/EAL, curriculum needs, AI, BYOD/personal devices, incidents and system limitations.
- Checks will be logged with date, tester, scope, outcome and action.

Access to monitoring data and alerts is restricted to authorised staff. Staff with access will receive appropriate safeguarding and data-protection training. Retention and access arrangements will be set out in relevant privacy information.

A Data Protection Impact Assessment (DPIA) will be completed before a new filtering/monitoring system is introduced or where a significant change is likely to create a high risk to individuals. Third-party provider privacy information will be reviewed as part of procurement and review.

Filtering is preventative and monitoring is reactive; neither replaces professional curiosity, active supervision or the duty of staff to report concerns.

- All staff will know how to report unsafe access, system failure, bypass attempts or unreasonable blocking.

5. Pupils with SEND and other vulnerabilities

- Online-safety teaching and reporting routes will be adapted to communication, cognition, sensory, physical, social, emotional or mental-health needs.
- Staff will avoid attributing concerning behaviour automatically to SEND and will consider online abuse, exploitation, bullying or coercion.
- Pupil voice and preferred communication methods will inform support and risk assessment.
- Reasonable adjustments or exceptions to device rules for medical, disability or safeguarding need will be documented and reviewed.

6. Curriculum and digital resilience

Online safety will be taught through computing, RSHE/PSHE and other relevant curriculum areas. Teaching will address privacy, online relationships, harmful content, misinformation, scams, cyber security, sexual imagery, deepfakes, AI, radicalisation, grooming, exploitation, reporting and help-seeking. It will be age-appropriate, evidence-informed and adapted where necessary.

7. Artificial intelligence

- Pupils may use generative AI only where a member of staff has authorised an age-appropriate educational use and appropriate safeguards are in place.
- School-approved tools will be preferred. Age restrictions and provider terms must be followed.
- Personal data, safeguarding information, confidential school information or special-category data must not be entered into public or unapproved AI tools.
- AI-generated work must not be presented as a pupil's own where this breaches assessment rules or teacher instructions.
- Deepfakes, sexualised AI imagery, impersonation, bullying, coercion or harmful AI-generated content will be treated as serious behaviour and, where relevant, safeguarding matters.

8. Mobile phones and smart technology

The College is a mobile-phone-free environment for pupils throughout the school day. Pupils must not access or use mobile phones or smart technology with equivalent functionality during lessons, movement time, break or lunch. Any exception must be authorised and documented for a specific medical, disability, safeguarding or other justified need. Storage, confiscation and sanctions are set out in the Behaviour/Acceptable Use arrangements.

9. Responding to online incidents

- Safeguarding concerns are reported to DSL/DDSL and recorded on CPOMS. Technical/security events may also be recorded in IT systems but safeguarding records must not be fragmented.

- Child-on-child online abuse, cyberbullying, sexual harassment and harmful sexual behaviour are handled under Child Protection and Behaviour procedures.
- Illegal content or suspected offences will be considered for police/other agency referrals using current safeguarding guidance.
- Evidence will not be deleted where it may be relevant to an offence; staff will not unnecessarily view or reproduce indecent imagery.
- Victims and alleged perpetrators will receive proportionate support and risk management.

10. Parents, carers and community

The College will communicate its online-safety expectations, filtering/monitoring arrangements, pupil AI expectations and routes for raising concerns. Parents/carers will be offered information and guidance and are expected to support the Acceptable Use arrangements.

11. Training, monitoring and review

- New staff receive online-safety training at induction; all staff receive at least annual updates within safeguarding training.
- DSL/DDSL knowledge is updated regularly and includes online safety. Governors receive appropriate safeguarding/online-safety training.
- The DSL will provide regular trend and incident assurance to the Headteacher and governors.
- This policy and the College online-safety risk assessment will be reviewed at least annually.

12. Related policies

- Child Protection Policy
- Safeguarding Policy
- ICT and Internet Acceptable Use Policy
- SEND Policy and SEN Information Report
- Behaviour Policy and mobile-phone arrangements
- Staff Code of Conduct
- Data Protection Policy and privacy notices
- Anti-bullying, RSHE/PSHE and curriculum policies
- Searching, screening and confiscation arrangements
- AI arrangements/policy where adopted

Sources used in drafting

- The Hayling College Child Protection Policy 2026/27 and September 2026 Hampshire model Safeguarding Policy supplied by the school.
- The Hayling College SEND Policy (reviewed/approved November 2025).
- The Key model Online Safety Policy (September 2026) and ICT and Internet Acceptable Use Policy (December 2025) supplied by the school.
- DfE Keeping Children Safe in Education 2026; statutory Mobile Phones in Schools guidance; DfE filtering and monitoring, digital technology and generative AI guidance current in September 2026.