Document Control
Reference: ICT Acceptable Use Policy
Version No: 1
Version Date: September 2026
Review Date: September 2026

THE HAYLING COLLEGE

Happy, Healthy, High Performing

ICT and Internet Acceptable Use Policy

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

Document Control
Reference: ICT Acceptable Use Policy
Version No: 1
Version Date: September 2026
Review Date: September 2026

THE HAYLING COLLEGE

Happy, Healthy, High Performing

1. Purpose and scope

ICT is integral to teaching, learning, safeguarding and administration. This policy sets rules for safe, lawful and responsible use of the College's ICT facilities and internet. It applies to staff, governors, pupils, volunteers, contractors, visitors and anyone authorised to use College systems.
This policy supersedes the College ICT Acceptable Use Policy dated January 2021 (reviewed June 2023). Its established safeguards on professional communications, social networking, personal devices, images/recording, confidentiality, monitoring, whistleblowing and the signed staff code of conduct have been retained or strengthened for the 2026/27 framework.

- Protect pupils and adults from safeguarding and online harms.
- Protect personal data, confidential information, systems and service continuity.
- Set clear expectations for professional and educational use.
- Support the Online Safety, Child Protection, Safeguarding, SEND, Behaviour and Data Protection policies.

2. Acceptable use principles

- Use College ICT primarily for education, College business or the authorised purpose of the user's role.
- Use only your own account and keep credentials secure; multi-factor authentication must be used where provided/required.
- Respect copyright, intellectual property, privacy and confidentiality.
- Use respectful language and behaviour online.
- Follow filtering, monitoring, security and software controls; do not attempt to bypass them.
- Report safeguarding, security, data-protection or technical concerns promptly.

3. Unacceptable use

- Illegal activity or advocacy of illegal activity.
- Bullying, harassment, stalking, discrimination, hate, sexual harassment or threatening/abusive communications.
- Accessing, creating, storing, sharing or linking to pornography, extreme violence, extremist/terrorist material or other illegal, offensive or harmful content except where specifically authorised for legitimate professional duties.
- Making, requesting, sharing or distributing nude/semi-nude or sexual imagery of children, including AI-generated or altered imagery.
- Online gambling, scams, phishing, financial fraud or deliberately unsafe activity.
- Unauthorised access, hacking, malware, denial-of-service activity, credential theft, bypassing filters, proxies/VPNs used to evade controls, or interference with systems.
- Installing unauthorised software/hardware or connecting devices without approval.
- Sharing confidential information or causing a data breach.

- Using ICT to damage the College's reputation or promote a private business without authorisation.
- Using AI contrary to section 8 of this policy.

4. Staff, governors, volunteers and contractors

Professional communication with pupils and parents/carers must take place through College-approved accounts and systems. Staff must not use personal email, personal messaging accounts or personal social-media accounts for routine College communication with pupils.

Staff must not accept or initiate social-media connections with current pupils. They must exercise professional judgement regarding former pupils, parents/carers and other members of the College community and ensure personal online activity does not compromise safeguarding, confidentiality, professional boundaries or confidence in the College.

Any attempt by a pupil to make inappropriate personal online contact with a member of staff must be reported to the DSL. Concerns about inappropriate ICT use by a colleague must be reported under safeguarding/low-level concern or whistleblowing procedures as appropriate.

Personal devices must not be used to take, store or transmit pupil images or confidential College information unless an exceptional, explicitly authorised arrangement is in place. College images and recordings must be created, stored, retained and deleted using approved systems.

- Use College-provided email/accounts for College business; do not use personal email for pupil or confidential College information.
- Do not share personal phone numbers or personal social-media accounts with pupils.
- Keep school devices secure, encrypted where supported, locked when unattended and updated. Report loss, theft, compromise or damage immediately.
- Do not store school-related personal data on unauthorised personal devices, personal cloud storage or removable media.
- Take photographs/video of pupils only on authorised equipment and for authorised purposes, in line with safeguarding and consent arrangements.
- Use remote access only through approved secure methods.
- Be aware that authorised monitoring of College systems may occur for safeguarding, security, legal and operational purposes.

5. Pupils

- Use College ICT and internet responsibly for learning and authorised school activities.
- Keep passwords private and never use another person's account.
- Do not attempt to access blocked, restricted or inappropriate content or bypass security controls.
- Tell a member of staff immediately about content, contact or activity that is upsetting, harmful, suspicious or unsafe.
- Do not bully, harass, impersonate, exploit or pressure others online, and do not create/share harmful or sexualised content.

- Use AI only when explicitly authorised by staff and in line with section 8.
- Understand that the College monitors use of its systems and that misuse may lead to proportionate sanctions and/or safeguarding action.

6. Mobile phones and personal smart devices

Pupils must not access or use mobile phones or smart technology with equivalent functionality at any point during the school day, including lessons, movement time, break and lunch. Devices brought to College must remain switched off and securely stored in accordance with the Behaviour Policy. Exceptions are only by explicit, documented authorisation for a specific medical, disability, safeguarding or other justified need. Misuse may result in confiscation and sanctions in line with the Behaviour Policy.

7. Data security and cyber security

Cyber security is a safeguarding concern as well as an IT and business-continuity concern because compromise of safeguarding, health or personal data may create direct risks to pupils.

The annual cyber assurance to FGB will report on the cyber risk assessment, MFA and privileged access, access reviews, patching/security updates, backups and restoration tests, incident-response/business-continuity testing, significant incidents and data breaches, supplier risks and outstanding improvement actions.

- The College will use appropriate firewalls, filtering, monitoring, anti-malware, authentication, access controls, encryption and backups.
- Strong unique passwords must be used. Staff must use the approved password-management approach and MFA where required.
- Access rights will follow least-privilege principles and be reviewed regularly.
- Software, operating systems and security updates will be applied promptly through managed processes.
- Critical data will be backed up on a regular managed schedule and recovery arrangements tested.
- A cyber risk assessment will be completed at least annually and reviewed during the year and after significant events or changes.
- The College will maintain and test an incident response/business continuity process, including communication routes if normal systems are unavailable.
- Users must report suspected phishing, malware, compromise, data breach or cyber attack immediately.

8. Artificial intelligence

- Only approved or expressly authorised AI tools may be used for College work or pupil learning.
- Provider age restrictions and terms must be followed. Pupil use must be supervised and educationally appropriate.
- Do not enter pupil personal data, safeguarding records, confidential information, special-category data, passwords or commercially sensitive material into public or unapproved AI systems.
- Check AI outputs for accuracy, bias, harmful content and suitability before use. Human professional judgement remains accountable.

- Do not use AI to impersonate others, create deepfakes/deep nudes, bully, harass, deceive, facilitate cheating or generate illegal/harmful content.
- Pupils must acknowledge AI assistance when required by staff and must not present AI-generated work as their own contrary to assessment rules.

9. Filtering, monitoring and privacy

The annual filtering and monitoring review will be undertaken by SLT, the DSL and IT support with the Safeguarding Governor involved in assurance. It will include documented checks on all relevant school-managed internet-connected devices and locations and will consider the pupil risk profile, including SEND/EAL, AI-generated/dynamic content, mobile/app content and use away from the College site.

Only authorised personnel may access monitoring information. The College will maintain appropriate retention arrangements, privacy information and DPIAs for monitoring systems and significant changes to them.

The College filters and monitors use of its ICT systems and network for safeguarding, security, legal compliance and operational purposes. This includes SENSO monitoring of pupil activity. Users should have no expectation that use of College systems is private beyond the protections required by law and College policy.

- Only authorised personnel may inspect or disclose monitoring information, and only for legitimate purposes.
- Safeguarding alerts are escalated to the DSL/DDSL; safeguarding decisions/actions are recorded on CPOMS.
- Filtering/monitoring failures or inappropriate blocking must be reported. No user may bypass controls without an approved, documented exception.
- Relevant privacy notices and data-protection impact assessments will cover monitoring systems where required.

10. Internet and Wi-Fi access

- Pupil internet access is filtered and monitored and is for authorised educational use.
- Staff access is subject to appropriate staff filtering/monitoring profiles.
- Guest/personal devices, where access is permitted, will use an appropriately segregated network.
- Wi-Fi credentials must not be shared with unauthorised users.

11. Misuse, sanctions and safeguarding

Responses will be proportionate to the circumstances and may include restriction/removal of access, confiscation, behaviour sanctions, staff disciplinary action, safeguarding action, data-breach response and/or referral to police or other agencies. A safeguarding response takes priority where a child may be at risk.

12. Monitoring and review

- The Headteacher and Helen Cox, Assistant Headteacher (AHT) / DSL, monitor implementation with IT support. The Safeguarding Governor, Erika Anders, provides FGB challenge and assurance.
- The Governing Body receives assurance on filtering/monitoring, cyber risk and significant incidents.
- This policy will be reviewed at least annually and after material legal, safeguarding or technology change.

Appendix A - Pupil Acceptable Use Agreement (KS3/KS4)

- I will use College ICT for learning and authorised activities and follow staff instructions.
- I will keep passwords private, use only my own account and protect personal information.
- I will not bypass filtering/monitoring, access harmful content, bully or harass others, or create/share sexual or abusive imagery.
- I will use AI only when a member of staff authorises it and will follow the College's AI rules.
- I will not access or use my mobile phone/smart device during the school day unless I have a documented exception.
- I will tell a trusted adult if I see or receive something harmful, unsafe or upsetting.
- I understand that College systems are monitored and misuse may lead to sanctions or safeguarding action.

Pupil name: _____ Signature: _____ Date: _____

Parent/carer: I have read and will support these expectations. Signature: _____ Date: _____

Appendix B - Staff/Governor/Volunteer/Visitor Acceptable Use Agreement

This agreement carries forward the professional-boundary and safeguarding expectations of the College's previous ICT Acceptable Use Policy. Staff are expected to read and sign it as confirmation that they understand and will follow the policy.

I will use College-approved communication channels with pupils and parents/carers and maintain appropriate professional boundaries in my personal use of social media.

I will report inappropriate online contact, safeguarding concerns, suspected misuse by pupils or colleagues, and accidental access to harmful material promptly through the appropriate safeguarding/IT route.

I understand that a breach may be managed under the Staff Code of Conduct or disciplinary procedures and may also require safeguarding, police or social-care referral.

- I will use College systems lawfully, professionally and for authorised purposes.
- I will protect credentials, devices, personal data and confidential information and report any loss, breach or compromise.
- I will not bypass security/filtering controls or install/connect unauthorised software or hardware.

- I will not input pupil personal data, safeguarding information or confidential school data into public/unapproved AI tools.
- I will report online safeguarding concerns to the DSL/DDSL and technical/security concerns through the agreed IT route.
- I understand that use of College systems is subject to lawful filtering and monitoring.

Name: _____ Role: _____ Signature: _____
Date: _____

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.