



ICT and AI Acceptable Use Policy

HBB-POL-08 | Academic Year 2026–27

Policy reference	HBB-POL-08
Version	2026–27 v1.0
Policy date	October 2026
Date of next review	August 2027
Policy owner	Headmaster
Policy lead	ICT Manager, with the Deputy Head (Academic) for AI in teaching and learning
Reviewed by	Leadership Team (LT) and Education and Safeguarding Committee
Approved by	Board of Governors
Intended audience	Pupils, parents, all staff and residents
Location	Staff Portal, Parent Portal, pupil portal and School website
Related policies	Safeguarding and Child Protection Policy (HBB-POL-01); Data Protection Policy (HBB-POL-09); Communication Policy (HBB-POL-10); Email Etiquette Policy (HBB-POL-11); Academic Honesty Policy; Behaviour Policy; Staff Code of Conduct

1. Purpose and scope

- 1.1 This policy sets out how technology, including artificial intelligence (AI), is used safely, lawfully and responsibly at Haileybury Bhaluka. Its purposes are to:
- keep the whole Haileybury Bhaluka community safe and well;
 - protect the reputation of Haileybury Bhaluka and its community;
 - make the most of the power of technology, including AI, for learning and collaboration;
 - help the school community use ICT to develop the skills to investigate, create, communicate, collaborate and organise; and
 - support Haileybury Bhaluka's contribution to local, national and international communities.
- 1.2 This policy applies equally to all members of the Haileybury Bhaluka community: pupils, staff, residents, Governors, visitors and parents (when using School systems or communicating with the School). It covers School-owned and personal devices whenever they are used on campus, on School activities, or to access School systems and accounts.
- 1.3 **Part A** covers ICT acceptable use. **Part B** covers artificial intelligence, with separate sections for staff, pupils and parents.

2. Definitions

- 2.1 In this policy:

- **Device** means any electronic tool used within the School. Devices may be owned by the School or personal. They will usually connect to a network (the School's wireless or cabled network, or a mobile 4G/5G network), but may not connect to any network in an obvious way, e.g. a digital camera, USB stick or external hard drive.
- **Cloud services** means online services managed by the School, such as Google Workspace for Education, Frog, Zoom and other approved platforms.
- **Social media** means applications, websites or platforms used for text or instant messaging, or for posting messages, status updates, videos, animations or photographs. This includes "closed" groups such as WhatsApp or Signal.
- **Artificial intelligence (AI)**, and in particular **generative AI**, means tools that can create text, images, audio, video or code in response to prompts (for example chatbots, image generators and AI features built into other apps).
- **Deepfake** means an image, video or audio recording that has been created or altered using AI to show a real person saying or doing something they did not say or do.

PART A: ICT ACCEPTABLE USE

3. ICT administration

- 3.1 Haileybury Bhaluka is committed to giving all staff and pupils the technology they need to best support teaching and learning. An age-appropriate ICT Use Agreement is shared with pupils every year to support safe and appropriate use of ICT at school.
- ICT procedures and guidelines are reviewed annually by the ICT Manager. All new employees read, accept and sign them.
 - The ICT Security Procedures give all employees a shared understanding of ICT use at Haileybury Bhaluka.
 - The Staff Guidelines for Information Safety support employees in the safe handling of physical and electronic information.

4. Acceptable use

- 4.1 Acceptable use of the Haileybury Bhaluka network means conducting ourselves, at all times, in ways that are **safe, legal, careful, ethical and mindful of the Haileybury Bhaluka community**.
- 4.2 In a busy boarding school there are times when you may use devices for personal reasons that are not educational or work-related. This is acceptable when you are not required to be engaged in School tasks, provided you follow this policy.
- 4.3 Devices may also be used for personal reasons after the school day, in your own accommodation at non-contact times, when travelling to or from a fixture, or where permitted for essential personal reasons during the school or working day. Acceptable use still applies whenever a device is used in, or brought into, school.

5. Unacceptable use

- 5.1 Unacceptable use includes viewing, creating, posting or commenting on content in the following categories:

Unsafe – for example:

- visiting sites that appear legitimate but are fake and try to trick you into sharing highly personal information (phishing);
- using a VPN or proxy server to get around the School's firewall and filtering. These systems are designed to keep you safe, and trying to bypass them is unsafe.

Illegal – for example:

- copyright infringement;
- fraud;

- radicalisation or extremist material;
- sending abusive, offensive or harassing material to or about others (cyberbullying), including on the grounds of race, nationality, ethnicity, religion or belief, sex, gender, sexuality, age or disability;
- creating, possessing or sharing nude or sexual images of anyone under 18, including AI-generated or altered images;
- attempting to hack into networks or accounts;
- posting or sharing false material about another person or organisation.

Careless – for example:

- posting or sharing material about an organisation or individual that may not be true, including misinformation and disinformation;
- commenting on a situation in a way that could easily be misunderstood, such as using sarcasm about a sensitive topic on X or Instagram;
- staff contacting pupils through personal email accounts, messaging apps or social media, or vice versa. This blurs the professional boundary between staff and pupils and is not permitted.

Unethical – for example:

- viewing obscene, inflammatory or pornographic content (which may also be illegal);
- failing to consider the needs of others in the way you use the network.

Not mindful of the community – for example:

- posting content that could harm the Haileybury Bhaluka community, such as unkind comments about other schools in a WhatsApp group, or anything that could bring the School into disrepute;
- disclosing personal information about others, or posting their images, without their consent.

5.2 The relevant law of Bangladesh includes the **Cyber Security Ordinance 2025** and the **Pornography Control Act 2012**. Serious breaches may be reported to the police.

6. Monitoring and filtering

- 6.1 The School does all it reasonably can to keep every member of the community safe. It therefore uses filtering and monitoring systems that block or flag potentially harmful, unethical or illegal content. These systems are designed in line with the DfE's filtering and monitoring standards and the online risks set out in KCSIE 2026: content, contact, conduct and commerce. This includes misinformation, disinformation, conspiracy theories, and AI-generated or altered images.
- 6.2 The School can monitor the use of School-supplied software and hardware, such as a School device or a School Google account, even when it is used off the School network, in another location or on a mobile network. If you are signed in to your @haileybury.com.bd account, the School can monitor your activity on connected services such as YouTube or Google Search, even on a different network. You can sign out of your School account on a personal device. The School cannot, and does not wish to, monitor your activity on accounts it has not provided. Whichever network you use, you are still a member of the Haileybury Bhaluka community, and we expect you to behave in a safe, legal, careful and ethical way.
- 6.3 Filtering and monitoring alerts that raise a safeguarding concern are passed immediately to the DSL. The ICT Manager reviews and tests the filtering and monitoring systems regularly and reports to the Online Safety Group.
- 6.4 Most data about pupils is personal or special category data under data protection law. How the School handles such data is set out in the Data Protection Policy.

7. Good practice

- 7.1 All users must:

- create a password that is memorable to them but hard to guess, and use two-factor authentication where it is available;
- never share their password with anyone else;
- log off or lock computers that others can easily access;
- avoid sharing personal devices, or at least avoid staying signed in on a device shared with someone else;
- report any breach of this policy to the ICT Manager (or, for safeguarding concerns, to the DSL), remembering that the purpose of this policy is to protect people;
- contact the ICT Manager if they are unsure about anything relating to the safe or acceptable use of devices.

8. Pupil ICT Use Agreement

8.1 Pupils and parents sign the ICT Use Agreement when the pupil joins the School and at the start of every academic year. Staff review and sign the Staff Guidelines for Information Safety and the ICT Security Procedures every year. The pupil agreement includes the following rules:

- 1) Recreational use of ICT devices in school is a privilege, not a right.
- 2) During lessons, ICT is used for learning and only as directed by a teacher.
- 3) ICT devices and access are used respectfully and responsibly.
- 4) Keep all personal information (yours and others') confidential online. Your user account is strictly personal.
- 5) Never share personal information (passwords, home address, telephone number, full name, etc.) online.
- 6) Show any member of staff what you are working on when asked during the school day.
- 7) If you have a technical problem, report it to the ICT Department or a member of staff.
- 8) If anything online makes you uncomfortable, tell a member of staff straight away.
- 9) ICT must never be used to threaten, harass or bully others, or to share pornographic, racist or other offensive material.
- 10) Use AI tools only as set out in Part B of this policy.

8.2 Inappropriate use of ICT includes:

- committing crimes;
- bullying, harassing or stalking others;
- copyright violations, such as illegally copying music, films, pictures or software (see the Academic Honesty Policy);
- sending obscene, hateful or threatening communications, or communicating or publishing inaccurate or offensive material;
- accessing someone else's files or reading their email without permission;
- lending your user identity or password to another person, or acquiring or using someone else's identity (if you think someone knows your password, you must change it immediately);
- playing electronic games unless approved by a teacher;
- visiting websites blocked by the School, or bypassing any School restrictions on internet access;
- downloading software without permission, or deliberately uploading or downloading a computer virus;
- buying or selling things online without permission;
- sending unsolicited advertising, junk mail, spam, chain letters or similar;
- viewing, downloading or uploading pornographic, violent or offensive images or stories;
- using someone else's identity to send messages, or giving other people's email addresses to any website;
- using chat services or social media during lessons without a teacher's permission;

- using the School network to try to access equipment or resources you have no right to access.

PART B: ARTIFICIAL INTELLIGENCE

9. Our approach to AI

- 9.1 Haileybury Bhaluka recognises that AI is changing how people learn, work and communicate. We want pupils to leave school as confident, critical and ethical users of AI, and we want staff to use AI to reduce workload and improve teaching, without losing the human relationships at the heart of a Haileybury education.
- 9.2 Our use of AI follows six principles:
- **Safety first:** AI use must never put pupils at risk. Safeguarding takes priority over convenience or innovation.
 - **Approved tools only:** School work involving pupils' or staff's data, or pupils' own use of AI in lessons, uses tools approved by the School.
 - **Protect personal data:** personal data is never entered into unapproved AI tools.
 - **Human oversight:** AI can support professional judgement but never replace it. A person is always responsible for any output that is used.
 - **Honesty and transparency:** we are open about when and how AI has been used.
 - **Critical thinking:** AI can be wrong, biased or out of date. Everything it produces must be checked.

10. Approved AI tools

- 10.1 The ICT Manager and the Deputy Head (Academic) keep a list of AI tools approved for use at Haileybury Bhaluka, published on the Staff Portal and pupil portal. A tool is only approved after its safety, age suitability, data protection (including a Data Protection Impact Assessment where personal data is involved) and filtering and monitoring arrangements have been checked.
- 10.2 Many AI tools set a minimum age of 13, and some of 18, and may require parental consent for users under 18. Pupils may only use AI tools that are appropriate for their age and approved by the School. Pupils under 13 use AI only through School-approved tools, under teacher direction.
- 10.3 AI features in approved platforms (for example Google Workspace for Education) are configured by the ICT Department with appropriate filtering, monitoring and age settings.

11. AI: guidance for staff

Staff may use approved AI tools to:

- plan lessons and generate resources, examples, questions and differentiated materials;
- draft or improve communications, reports and documents, which they then check and edit;
- support administrative tasks and data analysis that do not involve unapproved processing of personal data;
- support their own professional learning.

Staff must:

- use only School-approved tools for any work involving pupil, parent or staff information, and never enter personal data, safeguarding information or confidential School information into an unapproved AI tool;
- check all AI-generated content for accuracy, bias, suitability and copyright before using or sharing it. The member of staff remains responsible for anything they publish, send or teach;
- never rely on AI alone to mark, assess, write reports on, or make decisions about pupils (including on behaviour, admissions or safeguarding) or staff. Professional judgement must always be applied and recorded;

- be open with colleagues, pupils and parents about significant use of AI, e.g. where AI has substantially generated a resource or communication;
- teach and model the responsible, critical use of AI, and set clear expectations for each task about whether and how pupils may use AI;
- follow awarding body rules (Cambridge International, Pearson Edexcel and the International Baccalaureate) on AI in assessed coursework, and report suspected malpractice to the Exams Officer;
- report to the DSL immediately any safeguarding concern involving AI, including AI-generated nude or sexual images, deepfakes of pupils or staff, or pupils engaging with harmful AI chatbots.

Staff must not:

- use AI to create images, video or audio of real pupils, parents or colleagues, or upload pupils' photographs to AI tools;
- use AI tools to monitor or profile individual pupils, except through systems approved by the School;
- present AI-generated work as their own where that would be misleading, e.g. in professional qualifications or published writing.

12. AI: guidance for pupils

You may use AI to help you learn when your teacher allows it, for example to:

- explain an idea in a different way, or quiz yourself on a topic;
- brainstorm ideas, which you then develop yourself;
- get feedback on your own draft, which you then improve yourself;
- practise languages, coding or problem solving.

- 12.1 For each task, your teacher will tell you whether AI use is **not allowed**, **allowed for specific purposes**, or **encouraged**. If you are not sure, ask before you use it.

Academic honesty

- 12.2 Work you submit must be your own. Using AI to produce work and presenting it as your own is academic dishonesty, and will be dealt with under the Academic Honesty Policy.
- 12.3 Where AI use is allowed, you must acknowledge it: say which tool you used, what you asked it, and how you used the response.
- 12.4 In IGCSE, IB Diploma and other public examinations and coursework, you must follow the awarding body's rules on AI exactly. Misuse of AI in assessed work is malpractice and can lead to disqualification.

Staying safe with AI

- Use only School-approved AI tools that are suitable for your age.
- Never share personal information about yourself or anyone else with an AI tool, including names, photographs, addresses or passwords.
- Never create, request or share AI-generated or altered images, video or audio of real people, especially other pupils or staff. Creating or sharing a nude or sexual image of anyone under 18, including a fake one, is a crime and a serious safeguarding matter.
- Remember that AI chatbots are not people and are not friends or counsellors. If you are worried, upset or struggling, talk to a trusted adult: your HM, Tutor, the School Counsellor, the Medical Centre or the DSL.
- AI can make mistakes and can produce false or biased information. Always check important facts with reliable sources.
- If you see AI-generated content that worries you, or that shows someone you know, tell a member of staff straight away. You will be supported, not blamed.

13. AI: guidance for parents

How the School uses AI

- 13.1 The School uses approved AI tools to support teaching, learning and administration. Your child's personal data is only processed with approved tools, in line with the Data Protection Policy. Decisions about your child are always made by staff, never by AI alone.

How you can help at home

- Talk to your child about how they use AI, and encourage them to use it to learn, not to do their work for them.
- Check the age ratings and terms of any AI app your child uses, especially when they are at home at weekends and in the holidays.
- Talk to your child about the risks of deepfakes, AI-generated images and AI "companion" chatbots, and encourage them to tell you or the School if anything worries them.
- Please do not upload photographs or videos of other people's children to AI tools or social media.
- Support the School's expectations on academic honesty, particularly for coursework and public examinations.

Verifying communications from the School

- 13.2 AI can now be used to create convincing fake messages, voices and videos. The School will only contact you through official channels (see the Communication Policy). If you receive an unexpected request, especially one involving money, personal details or collecting your child, please check it with the School directly before acting.

14. Sanctions

- 14.1 Our aim is to take a firm but practical approach to breaches of this policy. The School has the right to confiscate a device for inspection, in line with the Searching and Confiscation Policy, and pupils must co-operate with staff in reasonable efforts to check for inappropriate stored content or access to inappropriate sites. Where a device may contain an indecent image of a child, staff must not view it but must refer the matter immediately to the DSL.
- 14.2 In some cases you may need support and guidance because you have stumbled into a difficult situation without meaning to. In others, you may have breached this policy through carelessness, or deliberately.
- 14.3 Sanctions for breaches of this policy are at the Headmaster's discretion, in line with the Behaviour Policy (for pupils) or the Disciplinary Procedures (for staff).
- 14.4 If the School's ICT resources are damaged or lost through deliberate action or negligence, the School may require compensation.
- 14.5 Compensation for loss of or damage to ICT equipment borrowed from the School (for example a laptop) is governed by a separate agreement between the pupil and the School.

15. On leaving the School

- 15.1 All School equipment must be returned. All software, documentation and data owned or licensed by the School must be deleted so that the pupil can no longer access it, unless a written agreement exists between the School and the copyright owners. The School reviews Google accounts each year in July. The accounts of pupils who have left, and all documents in them, are deleted. Pupils are told in advance so that they can save their own work.

16. CCTV

- 16.1 CCTV cameras are installed in common areas of the School premises for monitoring and recording. The Head of Security, main gate security and patrolling security staff act as CCTV operators. A CCTV operator's role is to:

- observe the CCTV and respond appropriately to ensure the safety and wellbeing of pupils, staff, visitors and School property;
- protect the School from risks such as robbery, theft and fraud by investigating activity seen and responding to emergencies;
- operate and monitor all CCTV systems professionally and efficiently;
- record all events and actions monitored from the control room clearly and accurately in writing;
- keep all information accurate and confidential.

16.2 Access to view CCTV is limited to designated staff appointed by the Headmaster. Permission to view recorded footage must be obtained from the Headmaster or the Head of Security, for a valid reason. CCTV is never installed in bedrooms, washrooms or changing areas. Footage is kept and deleted in line with the Data Retention Policy.

17. Confirmation of understanding

- 17.1 Staff sign: *"I confirm that I have read and understood the School's ICT and AI Acceptable Use Policy and agree to follow it. I understand that a breach of this policy may result in disciplinary action under the School's policies and procedures."*
- 17.2 Pupils sign: *"I have read and understood the ICT and AI Acceptable Use Policy and the ICT Use Agreement, including the rules on using AI. I agree to follow them and understand that breaking them may lead to sanctions."*
- 17.3 Parents sign: *"I have read the ICT and AI Acceptable Use Policy with my child, and I support the School's expectations, including those on artificial intelligence."*

18. Review record

Summary of changes (October 2026 review)

Area	Change made
Title and dates	Retitled "ICT and AI Acceptable Use Policy". Policy date October 2026 (the previous version was due for review in August 2026); next review August 2027. Owner changed to Headmaster, with the ICT Manager as lead.
Artificial intelligence (new)	New Part B on artificial intelligence: principles, approved tools, age limits, data protection and human oversight, and separate sections for staff, pupils and parents. Covers academic honesty and awarding body rules (Cambridge, Pearson Edexcel, IB), deepfakes and AI-generated nude images, AI chatbots and companions, and how to verify communications.
Safeguarding and KCSIE 2026	Filtering and monitoring now references the DfE filtering and monitoring standards and the online risks in KCSIE 2026 (content, contact, conduct and commerce, including misinformation, disinformation, conspiracy theories, and AI-generated and altered images). AI-generated nude images are a safeguarding matter, reported to the DSL.
Bangladesh law	The repealed "Digital Security Act" replaced with the Cyber Security Ordinance 2025 and other relevant law of Bangladesh.
Tidying	Duplicate list items removed (e.g. "commercial activities" appeared twice). Garbled sentence about technical problems corrected. Account deletion wording on leaving corrected. "G Suite" changed to Google Workspace and "Twitter" to X. Numbering fixed.
Agreements	Separate signed acknowledgements for staff, pupils and parents, including the AI sections.

Version history

Date	Version	Reviewed by	Notes
August 2025	2025-26	ICT Manager	Original ICT Acceptable Use Policy
October 2026	2026–27 v1.0	Headmaster (SOG)	Full review: dates, statutory references, roles and consistent Haileybury Bhaluka policy format

Approved by the Board of Governors	
Signed (Chair of Governors)	
Date	