Haileybury Bhaluka

ICT Acceptable Use Policy

Policy date:	August 2025
Date of next review:	August 2026
Owner:	ICT Manager
SLT committee to review:	LT
Intended audience:	Pupils, parents, and all staff
Location:	School portal and website

1. What are ICT Policies?

Policy is a set of principles or actions that guide the behavior of the school, its staff and its students. It bridges the gap between the vision and the plans that enable us to realise it.

2. Purpose of this policy

a. To keep the entire Haileybury Bhaluka community safe and well.

b. To preserve the reputation of Haileybury Bhaluka and its community.

c. To highlight the power of technology for learning and collaboration.

d. The school community will use ICT to develop the skills to investigate, create, communicate, collaborate, and organize.

e. Haileybury Bhaluka inspires actions and contributes to the local, national and international communities.

This policy, therefore, applies equally to all members of the Haileybury Bhaluka community: pupils, staff, and residents.

3. ICT Administration

Haileybury Bhaluka is committed to providing all staff and students with the technologically appropriate tools to best support teaching and learning. The grade level differentiated ICT user agreement is shared with students annually to support them with the safe and appropriate use of ICT at school.

- ICT-related procedures and guidelines are reviewed annually by administration, then read, accepted, and signed by all new employees.
- ICT Security Procedures: all employees have a common understanding of the ICT use at Haileybury Bhaluka.
- Staff Guidelines for Information Safety: These guidelines support employees with the safe use and treatment of physical and electronic information safety.

4. Definitions

a. In this policy, the term ‘device’ refers to any electronic tool used within the School.

b. Usually, such devices will be connected to a network of some sort - for example, the school wireless or cabled network. The devices may be owned by the School, or maybe personal devices, and it is possible that they are not connected to our network - for example, they connect to the internet via 4G/5G. They may not connect to any network in an obvious way - such as a digital camera, a USB stick, or an external hard drive.

c. ‘Cloud services’ are systems such as G Suite, Zoom, Notability, or one of the many other school-managed online services.

d. ‘Social media’ refers to communication applications, websites, or platforms that are used for text or instant messaging, or posting messages, status updates, videos, animations, or photographs. This can include ‘closed’ social media groups such as WhatsApp or Signal.

5. Acceptable use

Acceptable use of the Haileybury Bhaluka School network equates to conducting ourselves - at all times - in the following ways to ensure that it is: Safe, Legal, Careful, Ethical and Mindful of the Haileybury community

a. In a busy boarding school, there are times when you will be permitted to use electronic devices for personal reasons - reasons that are not educationally valid or work-related. This is of course acceptable when you are not required to be engaged in school-related tasks, during designated school hours, on the understanding that you are following the guidance above.

b. In situations, where electronic devices are used for personal reasons - for example after the school day has ended; when in your home during non-contact times; when off-site such as traveling to/from a fixture, or you may need to use a device where permitted for essential personal reasons during school or work time. Acceptable use nevertheless applies if a device is used in or brought into school.

6. Unacceptable use

a. We consider unacceptable use to be viewing, posting or commenting on content that falls under the following categories:

i. Unsafe - examples:

- Visiting sites that appear to be legitimate but which on reflection are fake, and are attempting to ensnare you into sharing highly personal information.

- Use of a VPN or proxy server to connect with other networks - the Haileybury Bhaluka Firewall and protection systems are designed to keep you safe. Attempting to use a VPN to bypass these is therefore something that is potentially unsafe.

ii. Illegal - examples:

- Copyright infringement

- Fraud

- Radicalisation

- Sending abusive, offensive, or harassing material to or about others (typically referred to as ‘cyber bullying’) - for example via Social Media - this includes any material which is abusive on the grounds of race, nationality, ethnicity, religion, belief, gender, sexuality, age or disability.

- Attempting to hack into networks.

- Posting or sharing false material about another person or organisation.

iii. Careless - examples:

- Posting or sharing material about another organization or individual which may not be true.

- Commenting on a situation in a way that could easily be misinterpreted - such as using sarcasm on a sensitive topic on Twitter or Instagram.

- Staff connecting with pupils via electronic means, such as personal email accounts, messages, or social media, and vice versa - this can potentially blur the professional boundary between staff and pupils.

iv. Unethical - examples:

- Viewing obscene, inflammatory or pornographic content - this might also be illegal, depending on the content.

- Failing to consider the needs of others in the way that you are using the Haileybury Bhaluka network

v. Oblivious to the needs of the Haileybury Bhaluka community - examples:

- Posting content that might impact negatively on the Haileybury community, such as unkind comments about other schools in a WhatsApp group, or which might bring the name of the School into disrepute

- Disclosing personal information about others in public without their consent

7. Monitoring

a. Our School does all that it reasonably can do in order to keep every member of our community safe. For this reason, we deploy software that monitors the use of our network and filters out content that is potentially harmful, unethical, or illegal.

b. If you use school-supplied software or hardware, then we are able to monitor the use of that - for example a school iPad, or access to Gmail. We can monitor the use of school-supplied software, such as Gmail, even if you use it outside of the school network, such as in a different location, or over a mobile phone network. Please be mindful that, if you are connecting to networks via other means, such as 4G or 5G mobile phone networks, you are still a member of the Haileybury Bhaluka community, and we still expect you to conduct yourself in a safe, legal, careful and ethical manner, and to be mindful of the needs of the wider Haileybury Bhaluka community. Further note that, if you are signed in to your @haileybury.com.bd Gmail account, we are able to monitor your activities on connected software services such as YouTube or Google searches, even if you are on a different network and in a different location. You can of course sign out of your Haileybury Bhaluka domain on your personal device, and we would not be able to nor wish to monitor your activities using an account other than a Haileybury Bhaluka - provided one. Please note that the majority of data relating to pupils in schools is considered to be either ‘personal’ or ‘sensitive’, under Data Protection law. How we handle such data is dealt with further in our Data Protection Policy.

8. Good practice

We require users to:

a. Create a password that is both memorable for the user and complex enough not to be guessed easily.

b. Avoid sharing their password with anybody else - this could lead to a potential security breach.

c. Ensure that they log off from computers that are easily accessible to other people.

d. Do not share personal devices with other people, or at the very least avoid being signed in to a device that is shared with somebody else.

e. If you need to report violations of this policy - remembering that the purpose of this policy is to protect people - then please get in touch with the ICT Manager.

f. Equally, if you are unsure about anything relating to the safe or acceptable use of devices within Haileybury Bhaluka, then please get in touch with the ICT Manager.

9. ICT Use Agreements

We have ICT Use Agreements for parents to refer to in our school. These are reviewed annually and are agreed upon and signed when the family joins the school and at the beginning of every school year.

In addition, the school has Staff Guidelines for Information Safety and ICT security procedures for the staff to review and sign every year.

1. Recreational use of ICT devices in school is a privilege, not a right.
2. ICT at school is for the purpose of learning and is only to be used with the direction of a teacher. Non-directed use is not permitted.
3. ICT devices and access at school are used respectfully and responsibly.
4. Keep all personal information (yours and others') confidential when working online. A user account is strictly personal.
5. Never share personal information (passwords, home address, telephone number, full name, etc.) online.
6. You must show any school staff what you are working on when requested during the school day.
7. If you have a technical problem with ICT, share Haileybury Bhaluka with the appropriate school staff.
8. If you encounter interactions using ICT that make you uncomfortable, tell a staff member at the school for support.
9. ICT resources may not be used to send threats, harass or bully others, spread pornographic or racist material, or for other acts that are in violation of the current Digital Security Act in Bangladesh.

10. Do not participate in any inappropriate use of ICT in school. Inappropriate use of ICT includes

    Committing crimes.

    Bullying, harassing, or stalking others.

    Committing copyright violations, such as illegal copying of music files, movies, pictures, or software, (As outlined in the Academic Honesty Policy).

    Transmitting obscene, hateful, or threatening communications.

    Communicating or publishing inaccurate or offensive materials,

    Invading someone else's private computer files or reading their Email.

    Lending a user identity or password to another person. It is not permitted to acquire another user's identity or use it. If a pupil suspects or knows that another person has learned his/her password, she or he is obliged to change it immediately.

    Playing electronic games unless approved by a teacher.

    Going on to websites that are blocked by the school.

    Downloading software from websites without teacher permission or approval.

    Uploading or downloading any computer virus on purpose.

    Engaging in commercial activities online such as buying or selling things, without permission from teachers.

    By-passing any school-imposed restrictions on internet access

    Transmitting via email any unsolicited advertising, promotional materials, "junk mail", "spam", "chain letters", "pyramid schemes", or any other form of E-mail solicitation.

    Engaging in commercial activities online such as buying or selling things, without permission from teachers.

    Viewing and/or downloading or uploading pornographic, violent or offensive pictures or stories.

    Using someone else’s identity to send an email, to a "Crush" or "Secret Admirer" website, or to any website collecting other people's email addresses for any purpose whatsoever.

    Engaging in the chat of any kind whether it is by using chatting programs or chatting rooms, including Facebook, and Gmail without explicit permission from the teacher.

    Using Haileybury Bhaluka ’s network to attempt to access equipment or resources they normally have no right to access.

10. Sanctions

a. Our aim is to take a firm but practical approach to dealing with breaches of this policy, where the School has the right to confiscate a device for inspection, and the student has a duty to cooperate with staff in their reasonable endeavours to check for inappropriate stored content or access to inappropriate sites.

b. In some circumstances, you might require support and guidance because you have inadvertently stumbled into a situation that you find difficult to extract yourself from.

c. In other circumstances, you might have breached this policy due to carelessness, or worse if your actions are deliberate.

d. Sanctions following a breach of this policy will be at the discretion of the Headmaster, in line with our School Behaviour, Rewards, and Sanctions Policy (for pupils) or our Disciplinary Procedures (for staff).

e. In the event of damage to or loss of Haileybury Bhaluka 's ICT resources, Haileybury Bhaluka may demand compensation from the pupil if the damage is due to willful intent or negligence

f. Compensation for loss of or damage to an assigned ICT resource (Laptop computer, for example) borrowed from the school is regulated by a separate agreement between the pupil and Haileybury Bhaluka .

g. Other sanctions may be employed in line with the **Haileybury Bhaluka** code of conduct.

11. On leaving school

- Any material belonging to Haileybury Bhaluka must be returned. All software, documentation, or data owned or lent by Haileybury Bhaluka must be deleted at the same time so it is no longer accessible to the pupil. Exemptions from the Haileybury Bhaluka rule only apply in cases where a written agreement exists between Haileybury Bhaluka and the copyright owners. The school reviews the existing Google accounts annually in July. Students not enrolled will have their account and all documents deleted during time spent at Haileybury Bhaluka.

12. CCTV monitoring

CCTV cameras are installed in various locations of Haileybury Bhaluka premises for monitoring and recording in the common area. There is no specific person for it so the Head of Security / Main Gate Security / Patrolling Security will play the role of CCTV operator.
A CCTV operator's role will be:

- To observe the CCTV and respond to situations appropriately to ensure the safety and wellbeing of all pupils, staff, visitors, and assets of Haileybury Bhaluka.
- Protecting the Haileybury Bhaluka from all kinds of risks such as robbery, theft, and fraud, by investigating activity seen and responding to emergencies.
- Operating and monitoring all CCTV systems and relevant tools in a professional and efficient way.
- Record all events and actions monitored from within the control room in clear and accurate written forms.
- Maintain the accuracy and confidentiality of all information,
- Access to view the CCTV is limited to designated personnel appointed by the Headmaster.
- Permission to view the CCTV footage must take from the school Headmaster, or Head of Security with valid reason.

13. Confirmation of Understanding

“I confirm that I have read and understand the School’s ICT Acceptable Use Policy and agree to adhere to it. I understand that a breach of this policy could result in disciplinary action under the School’s relevant policies and procedures.”