



Data Protection Policy

HBB-POL-09 | Academic Year 2026–27

Policy reference	HBB-POL-09
Version	2026–27 v1.0
Policy date	October 2026
Date of next review	August 2027
Policy owner	Headmaster
Policy lead	Chief Operating Officer (COO), Data Protection Lead
Reviewed by	Leadership Team (LT)
Approved by	Board of Governors
Intended audience	Staff, Governors, contractors and accreditation bodies
Location	Staff Portal, Governor Portal and School website
Related policies	Privacy Notice; Data Retention Policy; ICT and AI Acceptable Use Policy (HBB-POL-08); Safeguarding and Child Protection Policy (HBB-POL-01); Staff Code of Conduct; Complaints and Appeals Policy (HBB-POL-12)

1. Background

- 1.1 Haileybury Bhaluka is committed to meeting its legal obligations on data protection and to handling personal data fairly, lawfully and securely.
- 1.2 In the course of its activities, the School collects, stores and processes personal data, some of it sensitive, about staff, pupils, their parents, contractors and other third parties. As data controller, the School is liable for how its staff handle data. All staff therefore have a part to play in making sure the School complies with its legal obligations.
- 1.3 The School complies with the data protection law of Bangladesh, including the **Personal Data Protection Ordinance 2025**, which is regulated by the National Data Governance Authority. Some provisions of the Ordinance are being brought into force in phases, and the School will keep its procedures under review as they take effect. Under that law, the School acts as a *data fiduciary* (equivalent to a data controller).
- 1.4 As a British international school, Haileybury Bhaluka also follows the standards of the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018**, as amended by the **Data (Use and Access) Act 2025**, as best practice. The School is not regulated by the UK Information Commissioner's Office.

2. Definitions

- 2.1 Key data protection terms used in this policy are:

- **Data controller (data fiduciary):** a person or body that decides the purpose and means of processing personal data and is legally responsible for how it is used. The School is a data controller. An independent contractor who makes their own decisions about how they process data is also likely to be a data controller in their own right.
- **Data processor:** an organisation that processes personal data on behalf of a data controller, for example a payroll or IT provider, or another supplier with whom personal data may be shared but who may not decide how it is used.
- **Personal data breach:** a breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of, or access to, personal data.
- **Personal data (personal information):** any information relating to a living individual (a data subject) by which that individual can be identified. This is not just a name but any identifier, digital or contextual, including ID numbers, initials, job titles or nicknames. Personal data is created almost constantly in the ordinary course of work (for example in emails, notes and minutes of meetings). It includes opinions about the individual and any indication of the School's, or anyone's, intentions towards them.
- **Processing:** almost anything done with personal data, including obtaining or collecting it, structuring, analysing, storing or sharing it (internally or with third parties, including making it available to view electronically), altering it or deleting it.
- **Special categories of personal data:** data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health and medical conditions, sex life or sexual orientation, and genetic or biometric data used to identify an individual. Separate rules apply to personal data about criminal convictions and offences.

3. Application of this policy

- 3.1 This policy sets out the School's expectations and procedures for processing any personal data it collects from data subjects (including parents, pupils, employees, contractors and third parties).
- 3.2 Everyone who handles personal data as an employee or Governor of the School must comply with this policy. For employees, breaches of this policy may lead to disciplinary action. Accidental breaches of the law or of this policy will happen from time to time, for example through human error, and will not always be treated as a disciplinary issue. However, failure to report a breach that poses significant risks to the School or to individuals will be treated as a serious matter.
- 3.3 This policy also sets the standard expected of contractors who handle the School's personal data, whether they act as data processors on the School's behalf (in which case binding contract terms apply) or as data controllers in their own right.
- 3.4 Where the School shares personal data with other data controllers, such as other schools, parents or the relevant authorities, each party needs a lawful basis to process that data and is expected to do so lawfully, securely and confidentially, as set out in this policy.

4. Person responsible for data protection

- 4.1 The School has appointed the **COO** as its Data Protection Lead. The COO works to make sure that all personal data is processed in line with this policy and with applicable data protection law. Any questions about this policy, or concerns that it has not been followed, should be referred to the COO in the first instance, or by email to dataprotection@haileybury.com.bd.

5. The principles

- 5.1 Data protection law sets out principles for processing personal data, which data controllers and processors must follow. Personal data must be:
 - 1) processed lawfully, fairly and transparently;
 - 2) collected for specified, explicit and legitimate purposes, and used only for those purposes;
 - 3) adequate, relevant and limited to what is necessary for those purposes;
 - 4) accurate and kept up to date;

- 5) kept for no longer than necessary for the purposes for which it is processed; and
- 6) processed securely.

5.2 The wider "accountability" principle also requires the School not only to process personal data fairly and lawfully, but to be able to show that it does so. Among other things, this means:

- keeping records of our data processing activities, including logs and policies;
- documenting significant decisions and assessments about how we use personal data, including through Data Protection Impact Assessments (DPIAs); and
- generally keeping an audit trail on data protection and privacy matters, including when staff training took place, how and when consents were collected, and how personal data breaches were handled and whether (and to whom) they were reported.

5.3 The Board of Governors oversees the above through the Education and Safeguarding Committee. The COO is responsible for keeping these records up to date.

6. Lawful grounds for processing

6.1 Data protection law sets out several lawful grounds for processing personal data. One of these is consent. However, because of the high standard required for valid consent, and because consent can be withdrawn, the School prefers to rely on another lawful ground where it can.

6.2 One alternative is "legitimate interests", the most flexible basis for processing. It requires transparency and a balancing of the rights of the individual against the interests of the School. The School's legitimate interests are set out in its Privacy Notice.

6.3 Other lawful grounds include:

- compliance with a legal obligation, including in connection with employment, engagement of services, safeguarding and diversity;
- contractual necessity, e.g. to perform a contract with staff or parents, or to engage contractors;
- a narrower set of grounds for processing special categories of personal data (such as health information), which include explicit consent, emergencies and specific public interest grounds such as safeguarding.

6.4 Where the School relies on consent to process a child's personal data, it will obtain consent from a parent or guardian where the law requires.

7. Responsibilities of all staff

7.1 As stated above, all staff are responsible for making sure that the School processes data securely, fairly and lawfully.

Recording information accurately and appropriately

7.2 Personal data held by the School must be accurate, fair and adequate. Staff must tell the School if they believe any personal data is inaccurate or untrue, or if they are unhappy with how it is recorded. This applies to how staff record their own data and the personal data of others, in particular pupils, parents and colleagues, which must be recorded professionally and appropriately.

7.3 Staff should be aware that anyone they record information about (e.g. in emails or notes), whether digitally or on paper, may have the right to see it (see "Rights of individuals" below). This must not discourage staff from making necessary and sometimes difficult records of incidents or conversations involving colleagues or pupils, in line with the School's other policies, and there may sometimes be grounds to withhold such records from a request. Staff must make sure that every document or email they create is one they would be prepared to stand by if the person it concerns asked to see it. Staff should not put anything in writing that they would not be happy for a third party to read.

Data handling

7.4 All staff are responsible for handling the personal data they come into contact with fairly, lawfully, responsibly and securely, and in line with all relevant School policies and procedures.

The School requires all staff (and expects all contractors) to keep the data protection principles in mind and to make every effort to follow them whenever they process personal data.

- 7.5 Data protection affects many of the School's wider responsibilities, such as safeguarding and IT security, so all staff should read and comply with the following policies in particular:
- Safeguarding and Child Protection Policy
 - Staff Code of Conduct
 - ICT and AI Acceptable Use Policy
 - Equal Opportunities Policy
 - Dignity at Work Policy
- 7.6 Responsible processing also applies when creating new personal data or records, which must always be done fairly, lawfully, responsibly and securely.

Safeguarding and information sharing

- 7.7 Data protection law does not prevent the sharing of information for the purposes of keeping children safe. In line with KCSIE 2026, fears about sharing information must not stand in the way of safeguarding and promoting the welfare of children. Safeguarding information is shared on a relevant, necessary and proportionate basis, as set out in the Safeguarding and Child Protection Policy.

8. Data security and confidentiality

- 8.1 The School must make sure that appropriate security measures are in place against unlawful or unauthorised processing of personal data, and against accidental loss of or damage to it.
- 8.2 Data security is not only a digital issue. It also affects everyday processes such as filing and sending correspondence, including paper documents. Staff should always consider the safest means of storage and delivery, and what the consequences would be of loss or unauthorised access. No member of staff should give personal data about pupils or parents to third parties, including volunteers or contractors, without a lawful reason.

Paper documents

- 8.3 Staff must keep paper records securely in a locked area and dispose of them safely. Paper documents containing personal data must never be left unattended; they should be kept in a lockable filing cabinet or similar. They must not be put in general waste or recycling, but must be shredded. The School Office will securely dispose of documents for staff if needed.
- 8.4 To minimise the risk of loss, staff may not take paper records containing personal data off the School site, except where necessary in exceptional circumstances. Staff should not print documents containing personal data remotely. When transporting paper documents, staff must always keep them safe (e.g. when travelling on public transport).

Digital information

- 8.5 Staff must keep their devices, and the information accessible on them, secure at all times, in line with the ICT and AI Acceptable Use Policy. Staff must follow the ICT Department's advice on passwords, two-factor authentication and encryption, as issued from time to time.
- 8.6 Staff should consider the safety of, and access to, their devices when working both on site and remotely. For example, they should consider whether a screen or data on a device could be seen by a third party, or whether someone else could gain unauthorised access to the device (e.g. staff should not leave a device open and unattended in an unlocked office).
- 8.7 Staff must not use personal email accounts or unencrypted personal devices for official School business.

9. Artificial intelligence and personal data

- 9.1 Personal data about pupils, parents or staff must not be entered into any AI tool, chatbot or online service that has not been approved by the School for that purpose. Approved tools are listed by the ICT Manager, as set out in the ICT and AI Acceptable Use Policy.

- 9.2 Before any new AI tool, or other new technology, is used to process personal data, a Data Protection Impact Assessment must be completed and approved by the COO.
- 9.3 Decisions that significantly affect an individual (for example on admissions, assessment outcomes, discipline or employment) must never be made solely by automated means. A member of staff must always review and take responsibility for the decision.

10. Personal data breaches

- 10.1 Any actual or suspected personal data breach (for example an email sent to the wrong recipient, a lost device or document, or unauthorised access to a system) must be reported to the COO immediately, and in any event within 24 hours of discovery.
- 10.2 The COO will investigate, take steps to contain the breach, keep a record of it, and decide whether it must be reported to the regulator and/or the individuals affected, in line with applicable law. Safeguarding-related breaches are also reported to the DSL.

11. Management and training

- 11.1 The School expects everyone with management or leadership responsibilities to promote the principles above and to make sure that any concerns about how the School uses personal information are reported promptly to the COO. Managers and leaders should help to identify the need for regular staff training and put it in place. Staff must attend any data protection training the School requires.

12. Rights of individuals

- 12.1 As well as the School's responsibilities when processing personal data, individuals have specific rights. Perhaps the most significant is the right to access the personal data a data controller (i.e. the School) holds about them, known as the right to make a "subject access request". Such a request must be dealt with promptly. It does not need any particular form and does not need to mention the correct legislation. If you become aware of a subject access request, or any communication from an individual about their personal data, you must tell the COO as soon as possible. The School will carry out reasonable and proportionate searches to respond.
- 12.2 Individuals also have legal rights to:
- require the School to correct inaccurate personal data held about them;
 - ask the School to erase their personal data (in certain circumstances);
 - ask the School to restrict its processing (in certain circumstances);
 - receive the personal data the School holds about them in a commonly used format, so that it can be passed to another data controller; and
 - object, on grounds relating to their particular situation, to any processing they feel has a disproportionate impact on them.
- 12.3 None of these rights is unqualified, and exceptions may apply. However, certain rights are absolute and must be respected, specifically the right to:
- object to automated decision-making, including profiling (where a significant decision is made about someone without human involvement);
 - object to direct marketing; and
 - withdraw consent where the School relies on consent to process their personal data (without affecting the lawfulness of processing carried out before then, or of processing on a basis other than consent).
- 12.4 If you receive a request from anyone who appears to be exercising one or more of their data protection rights, you must tell the COO as soon as possible. Individuals who are unhappy with how the School has handled their data may complain under the Complaints and Appeals Policy or directly to the COO.

Appendix A: Handling data – get it right

This note is displayed in key locations around the site and online, to remind staff how to handle data fairly, safely and lawfully, and to promote best practice.

Protecting personal data is very important at Haileybury Bhaluka. In our day-to-day work we may all come across information about pupils, parents, staff or other people.

All staff are responsible for handling personal information fairly, lawfully and carefully. Ask yourself these questions when you are handling other people's personal data:

- Would I be happy if my personal information were used in this way? Would I expect it?
- Would I stand by how this information is recorded if the person concerned saw it?
- Is the way I am using or sending this information safe? Could it be lost or end up in someone else's hands?
- Am I about to put personal data into an AI tool or website that the School has not approved?
- What would the consequences be if I lost or misdirected this personal data?
- Am I disposing of this information securely? Could someone else take it?

Remember: if you are concerned about how we use anyone's personal information, or think there may have been a data breach, report it to the COO straight away, or email dataprotection@haileybury.com.bd.

13. Review record

Summary of changes (October 2026 review)

Area	Change made
Dates	Policy date October 2026 (the previous version was overdue for review, August 2024); next review August 2027.
Bangladesh law	Added Bangladesh's Personal Data Protection Ordinance 2025 and the role of the National Data Governance Authority. The School's role as data controller ("data fiduciary") under that law is set out.
UK law	UK GDPR and the Data Protection Act 2018 now referenced "as amended by the Data (Use and Access) Act 2025".
Breaches	Added a clear breach reporting procedure (report to the COO immediately and within 24 hours at the latest; the COO assesses whether notification is required).
AI	New section on artificial intelligence: no personal data in unapproved AI tools; a Data Protection Impact Assessment (DPIA) before any new AI tool is used with personal data; human oversight of decisions.
Consistency	"Bursar" corrected to COO. "Trustees" changed to Governors. The broken cross-reference to "section 5" fixed. "Computer Support Department" changed to ICT Department. Oversight by the Board of Governors through the Education and Safeguarding Committee.
Safeguarding	Added KCSIE 2026 wording: data protection law is not a barrier to sharing information to keep children safe.

Version history

Date	Version	Reviewed by	Notes
September 2023	2023-24	Headmaster	Original Data Protection Policy, reviewed by the Education Sub Committee

Date	Version	Reviewed by	Notes
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	