Data Protection Policy

Policy date:	September 2025
Date of next review:	November 2025
Owner:	Chief Financial and Operations Officer
Leadership Team:	Operations Leadership Team
Intended audience:	All Staff and Governors
Location:	School Portal, Governor Portal and website

1. Background

1.1 As a school, Haileybury must comply with important legal requirements relating to data protection.

1.2 During the course of the School's activities it collects, stores and processes personal data (sometimes sensitive in nature) about staff, pupils, their parents, its contractors and other third parties (as detailed more fully in the School's various Privacy Notices which are available on the School's website here). The School, as "data controller", is liable for the actions of its staff in how they handle data. It is therefore an area where all staff have a part to play in ensuring the School complies with its legal obligations.

1.3 UK data protection law consists primarily of the UK version of the General Data Protection Regulation (the GDPR) and the Data Protection Act 2018 (DPA 2018). The DPA 2018 includes specific provisions of relevance to independent schools: in particular, in the context of safeguarding obligations, and regarding the right of access to personal data.

1.4 Data protection law has in recent years strengthened the rights of individuals and placed tougher compliance obligations on organisations including schools that handle personal information. The Information Commissioner's Office (ICO) is responsible for enforcing data protection law, and will typically look into individuals' complaints routinely and without cost, and has various powers to take action for breaches of the law.

2. Definitions

2.1 Key data protection terms used in this policy are:

- **Data controller** – a person or body that determines the purpose and means of the processing of personal data, and who is legally responsible for how it is used. For example, the School is a data controller. An independent contractor who makes their own decisions about how they process data is also, separately, likely to be a data controller.
- **Data processor** – an organisation that processes personal data on behalf of a data controller, for example a payroll or IT provider or other supplier of services with whom personal data may be shared but who is not authorised to make any decisions about how it is used.
- **Personal data breach** – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- **Personal information (or 'personal data')** - any information relating to a living individual (a data subject) by which that individual may be identified by the controller. That is not simply a name but any form of identifier, digital or contextual, including unique ID numbers, initials, job titles or nicknames. Note that personal information will be created almost constantly in the ordinary course of work duties (such as in emails, notes, and minutes of meetings). The definition includes expressions of opinion about the individual or any indication of the School's, or any person's, intentions towards that individual.
- **Processing** – virtually anything done with personal information, including obtaining or collecting it, structuring it, analysing it, storing it, sharing it internally or with third parties (including making it available to be viewed electronically or otherwise), 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, genetic or biometric data used to identify an individual. There are also separate rules for the processing of personal data relating to criminal convictions and offences.

3. Application of this policy

3.1 This policy sets out the School's expectations and procedures with respect to processing any personal data we collect from data subjects (including parents, pupils, employees, contractors and third parties).

3.2 Those who handle personal data as employees or trustees of the School are obliged to comply with this policy when doing so. For employees, breaches of this policy may result in disciplinary action. Accidental breaches of the law or this policy in handling personal data will happen from time to time, for example by human error, and will not always be treated as a disciplinary issue. However, failure to report breaches that pose significant risks to the School or individuals will be considered a serious matter.

3.3 In addition, this policy represents the standard of compliance expected of those who handle the School's personal data as contractors, whether they are acting as "data processors" on the School's behalf (in which case they will be subject to binding contractual terms) or as data controllers responsible for handling such personal data in their own right.

3.4 Where the School shares personal data with third party data controllers – which may range from other schools, to parents, to appropriate authorities – each party will need a lawful basis to process that personal data, and will be expected to do so lawfully and with due regard to security and confidentiality, as set out in this policy.

4. Person responsible for Data Protection at the School

4.1 The School has appointed the Chief Financial and Operations Officer as the Data Protection Lead who will endeavour to ensure that all personal data is processed in compliance with this Policy and the principles of applicable data protection legislation. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred to the Chief Financial and Operations Officer.

5. The principles

5.1 The GDPR sets out six principles relating to the processing of personal data which must be adhered to by data controllers (and data processors). These require that personal data must be:

1) Processed **lawfully, fairly** and in a **transparent** manner;
2) Collected for **specific and explicit purposes** and only for the purposes it was collected for;
3) **Relevant** and **limited** to what is necessary for the purposes it is processed;
4) Accurate and kept up to date;
5) **Kept for no longer than is necessary** for the purposes for which it is processed; and
6) Processed in a manner that ensures **appropriate security** of the personal data.

5.2 The GDPR's broader 'accountability' principle also requires that the School not only processes personal data in a fair and legal manner but that we are also able to *demonstrate* that our processing is lawful. This involves, among other things:

- keeping records of our data processing activities, including by way of logs and policies;
- documenting significant decisions and assessments about how we use personal data (including via formal risk assessment documents called Data Protection Impact Assessments); and
- generally having an 'audit trail' vis-à-vis data protection and privacy matters, including for example when and how our Privacy Notice(s) were updated; when staff training was undertaken; how and when any data protection consents were collected from individuals; how personal data breaches were dealt with, whether or not reported (and to whom), etc.

The School has a Data Committee which oversees the above, and the Chief Financial and Operations Officer is responsible for keeping these records up to date.

6. Lawful grounds for data processing

6.1 Under the GDPR there are several different lawful grounds for processing personal data. One of these is consent. However, given the relatively high bar of what constitutes consent under GDPR (and the fact that it can be withdrawn by the data subject) it is considered preferable for the School to rely on another lawful ground where possible.

6.2 One of these alternative grounds is 'legitimate interests', which is the most flexible basis for processing. However, it does require transparency and a balancing assessment between the rights of the individual and the interests of the School. The School's legitimate interests are set out in its Privacy Notice, as GDPR requires.

6.3 Other lawful grounds include:

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

7. Responsibilities of all staff

As stated above, all staff have a responsibility to ensure that the School processes data securely, fairly and lawfully. The School will display the reminder notice in Appendix A in key locations to help staff remember the key principles set out below:

7.1 Recording information accurately and appropriately

It is important that personal data held by the School is accurate, fair and adequate. Staff are required to inform the School if they believe that *any* personal data is inaccurate or untrue or if they are dissatisfied 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 – in a way that is professional and appropriate.

Staff should be aware of the rights set out below, whereby any individuals about whom they record information (e.g. in emails or notes) digitally or in hard copy, may have the right to see that information. This must not discourage staff from making necessary and sometimes difficult records of incidents or conversations involving colleagues or pupils, in accordance with the School's other policies, and grounds may sometimes exist to withhold these from such requests. **However, staff must ensure that every document or email they create is in a form they would be prepared to stand by should the person about whom it was prepared ask to see it. Staff should not put anything in writing they would not be happy for a third party to read.**

7.2 Data handling

All staff have a responsibility to handle the personal data which they come into contact with fairly, lawfully, responsibly and securely and in accordance with all relevant School policies and procedures (to the extent applicable to them). The School requires all School staff (and expect all our contractors) to remain mindful of the data protection principles (see section 5 above), and to use their best efforts to comply with those principles whenever they process personal information.

In particular, there are data protection implications across a number of areas 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 Acceptable Use Policy
- Equal Opportunities Policies
- Dignity at Work Policy

Responsible processing also extends to the creation and generation of new personal data or records, as above, which should always be done fairly, lawfully, responsibly and securely.

7.3 Recording and reporting data breaches

One of the key obligations contained in the GDPR is on reporting personal data breaches. Data controllers must report certain types of personal data breach (those which risk an impact to individuals) to the ICO within 72 hours.

In addition, data controllers must notify individuals affected if the breach is likely to result in a "high risk" to their rights and freedoms. In any event, the School must keep a record of any personal data breaches, regardless of whether it needs to notify the ICO. If staff become aware of a personal data breach they must notify the Chief Financial and Operations Officer immediately. If staff are in any doubt as to whether to report something internally, it is always best to do so. A personal data breach may be serious, or it may be minor; and it may involve fault or not; but the School always needs to know about them to make a decision.

As stated above, the School may not need to treat the incident itself as a disciplinary matter – but a failure to report could result in significant exposure for the School, and for those affected, and could be a serious disciplinary matter whether under this policy or the applicable staff member's contract.

7.4 Data security and confidentiality

The School must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

Data security is not simply an online or digital issue but one that affects daily processes such as filing and sending correspondence, including hard copy documents. Staff should always consider what the most assured and secure means of storage and delivery is, and what the consequences would be of loss or unauthorised access. No member of staff should provide personal data of pupils or parents to third parties, including a volunteer or contractor, unless there is a lawful reason to do so.

Hard copy documents

Staff must keep any hard copy data safely, in a locked area, and must dispose of data safely and securely - **hard copy documents containing personal data should never be left in an area unattended but should be kept in a lockable filing cabinet or similar. Hard copies should not be placed in general waste or recycling, but should be shredded.** The School Office will securely dispose of hard copy documents for staff if needed.

To minimise risk of loss, staff are not permitted to remove hard copy personal data from the School site except where necessary in exceptional circumstances. Staff should not print documents containing such data remotely. When transporting hard copy documents, staff should always take care to keep them safe (e.g. when travelling on public transport).

Digital information

Staff must at all times ensure the security of their devices and the information accessible on them, in accordance with the School's ICT Acceptable Use Policy. Staff should ensure that they follow the Computer Support Department's recommendations for the protection of passwords, the use of two-factor authentication, and any methods relating to the encryption of data, as advised to staff from time to time.

Staff should consider the safety of, and access to, their devices when working both on site and remotely. For example, staff should consider whether a screen or data on a device might be visible to a third party, or whether another person may be able to have unauthorised access to that device (e.g. staff should not leave any device open and unattended in an unlocked office).

The use of personal email accounts or unencrypted personal devices by staff for official School business is not permitted.

7.5 **Management and training**

The School expects all those with management or leadership responsibilities to promote the above principles and to oversee the swift reporting of any concerns about how personal information is used by the School to the Chief Financial and Operations Officer. Those in management and leadership positions should help to identify the need for (and implement) regular staff training. Staff must attend any training the School requires of them.

8. Rights of individuals

8.1 In addition to the School's responsibilities when processing personal data, individuals have certain specific rights, perhaps most significantly that of access to their personal data held by a data controller (i.e. the School). This is known as the 'subject access right' (or the right to make 'subject access requests'). Such a request must be dealt with promptly and does not need any formality, nor to refer to the correct legislation. If you become aware of a subject access request (or indeed any communication from an individual about their personal data), you must tell the Chief Financial and Operations Officer as soon as possible.

8.2 Individuals also have legal rights to:

- require the School to correct the personal data held about them if it is inaccurate;
- request that the School erases their personal data (in certain circumstances);
- request that the School restricts its data processing activities (in certain circumstances);
- receive from the School the personal data it holds about them for the purpose of transmitting it in a commonly used format to another data controller; and
- object, on grounds relating to their particular situation, to any of the School's particular processing activities where the individual feels this has a disproportionate impact on them.

8.3 None of the above rights for individuals are unqualified and exceptions may well apply. However, certain rights are absolute and must be respected, specifically the right to:

- object to automated individual decision-making, including profiling (i.e. where a significant decision is made about the individual without human intervention);
- object to direct marketing; and
- withdraw one's consent where the School is relying on it for processing their personal data (without affecting the lawfulness of processing carried out prior to that point in reliance on consent, or of any processing carried out on some other legal basis other than consent).

8.4 In any event, however, if you receive a request from an individual who is purporting to exercise one or more of their data protection rights, you must tell the Chief Financial and Operations Officer as soon as possible.

9. Processing of financial and payment information

9.1 The School complies with the requirements of the PCI Data Security Standard (PCI DSS).

Staff who are required to process payment card data must ensure that they are aware of and comply with the most up to date PCI DSS requirements. If you are unsure in this regard please seek further guidance from the Head of Finance or the Chief Financial and Operations Officer.

Other categories of financial information, including bank details and salary, or information commonly used in identity theft (such as national insurance numbers or passport details) can also have material impact on individuals should they be lost or misused. Such information should be handled carefully and securely, and in accordance with this policy.

APPENDIX A

This note will be displayed in key locations on site and digitally, to remind staff how to handle data fairly, safely and lawfully, and to promote best practice.

Handling data - get it right

Protecting personal data is very important at Haileybury. We may all come across information belonging to pupils, parents, staff or other individuals in our day to day work.

All staff have a responsibility to handle 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 own personal information were being used in this way? Would I expect it?*
- *Would I stand by how I have recorded this information, if the person concerned was able to see it?*
- *Is the way I am using or sending this information safe? Could it be lost or end up in someone else's hands?*
- *What would be the consequences 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, report it to the Chief Financial and Operations Officer straight away, or email dataprotection@haileybury.com

Version history		
Date	**Reviewed by**	**Notes**
April 2022	Data Committee	New policy
April 2022	SLT	Approved
September 2025	Executive Leadership Team	Updated to reflect CFOO role