Mill Hill
EDUCATION GROUP

Data Protection Policy

Instilling values, inspiring minds

Mill Hill EDUCATION GROUP

Instilling values, inspiring minds.

Data Protection Policy

Contents

1. Introduction

The Mill Hill Education Group (the 'Group') is the trading name of The Mill Hill School Foundation and is a group of independent mainstream Schools which together educate girls and boys aged 6 months to 19 years. It currently comprises:

Senior Schools (Day and Boarding)
Mill Hill School
Mill Hill International
Cobham Hall
Heathfield School

Pre-Preparatory/Preparatory Schools (Day)
Grimsdell, Mill Hill Pre-Preparatory School*
Lyonsdown School*
Keble Prep*
St Joseph's in The Park*
Belmont, Mill Hill Preparatory School

All Through Schools
Abbot's Hill School (age 6 months to GCSE)*
Kingshott School (age 3 to GCSE)*
Westbrook Hay School (age 3 to GCSE)
*Schools with EYFS provision

This Policy applies to all Schools in the Group, including Early Years Foundation Stage (EYFS) settings. This Policy is published on the Schools' websites and is available in hard copy on request. The term 'School' in this Policy shall refer to each of the Group Schools, as appropriate.

The Mill Hill School Foundation is a Registered Charity. Both the Mill Hill School Foundation and Mill Hill School Enterprises are Companies Limited by Guarantee, employing both teaching and non-teaching staff. Legal responsibility rests with the Companies acting by the Court of Governors. The Head Teachers have day to day responsibility for the management of the Schools and the care of their Pupils.

Data protection is an important legal compliance issue for the Group. During the course of the Group's activities it collects, stores and processes personal data (sometimes sensitive in nature) about Staff, Pupils, their Parent/s/Guardian/s/Carer/s, its Contractors and other Third Parties (in a manner more fully detailed in the Group's Privacy Notice, which can be found on the Group website. The Group, as "Data Controller", is liable for the actions of its Staff and Governors in how they handle data. It is therefore an area where all Staff have a part to play in ensuring we comply with and are mindful of our legal obligations, whether that personal data handling is sensitive or routine.

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 our safeguarding obligations, and regarding the right of access to personal data.

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

Key data protection terms used in this Data Protection 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 Group (including by its Governors) is a Controller. An independent contractor who makes their own decisions 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 of calls, and minutes of meetings). The definition includes expressions of opinion about the individual or any indication of the Group'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

This Policy sets out the Group's expectations and procedures with respect to processing any 'personal data' it collects from 'data subjects' (including Parent/s/Guardian/s/Carer/s, Pupils, Employees, Contractors and Third Parties).

Those who handle personal data as Employees or Governors of the Group 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 Group or individuals will be considered a serious matter.

In addition, this Policy represents the standard of compliance expected of those who handle the Group's ' 'Personal Data' as Contractors, whether they are acting as 'Data Processors' on the Group'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.

Where the Group shares 'Personal Data' with 'Third Party Data Controllers' – which may range from other Schools, to Parent/s/Guardian/s/Carer/s, to appropriate Authorities, to Casual Workers and Volunteers – 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.

If you are a Volunteer [or Contractor], you will be a 'Data Controller' in your own right, but the same legal regime and best practice standards set out in this Policy will apply to you by law.

4. Person Responsible for Data Protection at the Group

The Group has appointed Maxine Zeltser as the Compliance Manager and Data Protection Co-Ordinator 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 in the first instance to the Data Protection Co-Ordinator who can be contacted by emailing compliance@millhill.org.uk.

5. The Principles

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:

Processed **lawfully, fairly** and in a **transparent** manner.

1. Collected for **specific and explicit purposes** and only for the purposes it was collected for.
2. **Relevant** and **limited** to what is necessary for the purposes it is processed.
3. **Accurate** and kept **up to date.**
4. **Kept for no longer than is necessary** for the purposes for which it is processed.
5. Processed in a manner that ensures **appropriate security** of the 'Personal Data'.

The GDPR's broader 'Accountability' Principle also requires that the Group not only processes 'Personal Data' in a fair and legal manner but that it is also able to *demonstrate* that its processing is lawful. This involves, among other things:

- Keeping records of its data processing activities, including by way of Logs and Policies.
- Documenting significant decisions and assessments about how it uses 'Personal Data' (including via formal risk assessment documents called 'Data Protection Impact Assessments').
- Generally having an 'audit trail' vis-à-vis Data Protection and Data Privacy matters, including for example when and how its 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.

6. Lawful Grounds for Data Processing

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 Group to rely on another lawful ground where possible.

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 Group. It can be challenged by 'Data Subjects' and also means the Group is taking on extra responsibility for considering and protecting people's rights and interests. The Group's legitimate interests are set out in its Privacy Notice, as GDPR requires.

Other lawful grounds include:

a. Compliance with a legal obligation, including in connection with employment, engagement of services and diversity.
b. Contractual necessity, e.g. to perform a Contract with Staff or Parent/s/Guardian/s/Carer/s or the engagement of Contractors.
c. 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. Headline Responsibilities of all Staff Record-Keeping

It is important that 'Personal Data' held by the Group is accurate, fair and adequate. Staff are required to inform the Group 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 Colleagues, Pupils and their Parent/s/Guardian/s/Carer/s – 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 on Group business (notably in emails and notes) digitally or in hard copy files may have the right to see that information. This absolutely must not discourage Staff from recording necessary and sometimes difficult records of incidents or conversations involving Colleagues or Pupils, in accordance with the Group's other Policies, and grounds may sometimes exist to withhold these from such requests. However, the starting position for Staff is to **record every document or email in a form they would be prepared to stand by should the person about whom it was recorded ask to see it**.

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 the Staff Handbook and all relevant Group Policies and Procedures (to the extent applicable to them). In particular, there are data protection implications across a number of areas of the Group's wider responsibilities such as safeguarding and IT

security, so all Staff should read and comply with the following Policies:

a. Safeguarding and Protecting the Welfare of Pupils Policy.
b. Acceptable Use of IT Policy/Agreement.
c. Online Safety Policy.
d. Staff Code of Conduct.

Responsible processing also extends to the creation and generation of new 'Personal Data / records, as above, which should always be done fairly, lawfully, responsibly and securely.

Avoiding, mitigating and reporting data breaches

One of the key obligations contained in the GDPR is reporting 'Personal Data' breaches. 'Data Controllers' must report certain types of 'Personal Data' breach (those which risk an impact on 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 Group 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 Maxine Zeltser, the Data Protection Co-Ordinator by emailing compliance@millhill.org.uk, or the compliance email address of their own School, as soon as possible.

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 Group always needs to know about them to make a decision.

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

Care and Data Security

More generally, the Group requires all its staff (and expects all its contractors) to remain mindful of the 'Data Protection Principles' (see section 3 above), and to use their best efforts to comply with those Principles whenever they process personal information. Data security is not simply an online or digital issue but one that affects daily processes: filing and sending correspondence, notably hard copy documents. 'Data Handlers' should always consider what the most assured and secure means of delivery is, and what the consequences would be of loss or unauthorised access.

The Group expects all those with management / leadership responsibilities to be particular champions of these Principles and to oversee the swift reporting of any concerns about how personal information is used by the Group to Maxine Zeltser, Compliance Manager and Data Protection Co-Ordinator, and to identify the need for (and implement) regular Staff training. Staff must attend any training the Group requires them Rights of Individuals

8. Rights of Individuals

In addition to the Group'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 Group). 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 inform the Compliance Manager and Group Data Protection Co-ordinator, Maxine Zeltser, by emailing compliance@millhill.org.uk, or your School's compliance email address, as soon as possible.**

Individuals also have legal rights to:

e. Require the Group to correct the 'Personal Data' we hold about them if it is inaccurate.
f. Request that the Group erases their 'Personal Data' (in certain circumstances)'
g. Request that the Group restricts its data processing activities (in certain circumstances).
h. Receive from the Group, the 'Personal Data' that it holds about them for the purpose of transmitting it in a commonly used format to another 'Data Controller'.
i. Object, on grounds relating to their particular situation, to any of the Group's particular processing activities where the individual feels this has a disproportionate impact on them'

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:

j. Object to automated individual decision-making, including profiling (i.e. where a significant decision is made about the individual without human intervention).
k. Object to direct marketing.
l. Withdraw one's consent where the Group 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).

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 Maxine Zeltser, the Data Protection Co-Ordinator, as soon as possible.

9. Data Security: Online and Digital

The Group 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. Staff should refer to the Staff Code of Conduct, and Acceptable Use of IT Policy/Agreement for details of their obligations.

10. Processing of Financial Data

Financial information, including bank details and salary, or information commonly used in identity theft (such as national insurance numbers or passport details) may not be treated as legally sensitive but can have a material impact on individuals and should be handled accordingly.

11. Review

This Policy shall be reviewed every two years or following any concerns, and/or updates to national guidance or procedures.

Last Review August 2025
Next Review August 2027

This Policy was approved by the Executive Team on 29 August 2025.

Instilling values, inspiring minds.

Mill Hill
EDUCATION GROUP

The Mill Hill Education Group is the brand name for The Mill Hill School Foundation.
Registered in England: number 3404450
Registered office: Walker House, Millers Close, The Ridgeway, Mill Hill, London NW7 1AQ
Registered charity number: 1064758.