Haberdashers' Monmouth Schools

Data Protection Policy

Appendix 1 - Storage & Retention of Records and Documents
Appendix 2 - Email Protocol

For the purpose of this policy 'the School' refers to the Haberdashers' Monmouth Schools (HMS).

Data protection is an important legal compliance issue for HMS. 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 (in a manner more fully detailed in the school's Privacy Notice). The school, as "data controller", is liable for the actions of its staff and 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.

The law changed on 25 May 2018 with the implementation of the General Data Protection Regulation (**GDPR**) – an EU Regulation that is directly effective in the UK, regardless of Brexit status – and a Data Protection Act 2018 (DPA 2018) was also passed to deal with certain issues left for national law. The DPA 2018 included 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.

Without fundamentally changing the principles of data protection law, and while providing some helpful new grounds for processing certain types of personal data, in most ways this new law has 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.

1. Introduction

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 school (including by its governors) is a controller. An independent contractor who makes their own such 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 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.

2. Application of this policy

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

Those who handle personal data as employees or governors 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 a disciplinary issue. However, failure to report breaches that pose significant risks to the school or individuals will be considered a serious matter.

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.

Where the school shares personal data with third party data controllers – which may range from other schools, to parents, 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.

GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Legal and secure information sharing between schools, children's social care and other local agencies is essential for keeping children safe and ensuring they get the support they need.

3. Person responsible for Data Protection at the School

The school has appointed the Foundation Bursar as the Data Protection Officer who will endeavour to ensure that all personal data is processed in compliance with this Policy and the principles of the GDPR. 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 Officer.

4. 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:

1. Processed **lawfully, fairly** and in a **transparent** manner;
2. Collected for **specific and explicit purposes** and only used 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.

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.

5. Lawful grounds for data processing

Under the GDPR there are several different lawful grounds for processing personal data. One of these is consent. However, because the definition of what constitutes consent has been tightened 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.

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

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.

6. Headline responsibilities of all staff

Record-keeping
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 you 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 parents – 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 school 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 school'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**.

All staff should comply with the Storage and Retention of Records and Documents document at Appendix 1.

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). 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:

- E-Safety and Safer Practice with Technology Policy

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 new 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 we need to notify the ICO. If staff become aware of a personal data breach they must notify the Foundation Bursar. 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.

Care and data security
More generally, we require all school staff (and expect all our 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 effects daily processes: filing and sending correspondence, notably hard copy documents.

We expect 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 school to the Foundation Bursar, and to identity the need for (and implement) regular staff training. Staff must attend any training we require them to.

7. Rights of Individuals

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 Foundation Bursar as soon as possible.

Individuals also have legal rights to:

- require us to correct the personal data we hold about them if it is inaccurate;
- request that we erase their personal data (in certain circumstances);
- request that we restrict our data processing activities (in certain circumstances);
- receive from us the personal data we hold about them for the purpose of transmitting it in a commonly used format to another data controller. It is acknowledged there is no secure exchange mechanism to do this for independent schools;
- object, on grounds relating to their particular situation, to any of our particular processing activities where the individual feels this has a disproportionate impact on them; and

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 we are 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 the Foundation Bursar as soon as possible.

8. Data Security: online and digital

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

- no member of staff is permitted to remove personal data from school premises, whether in paper or electronic form and wherever stored, without prior consent of Principal or Bursar.
- 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.
- Where a worker is permitted to take data offsite on memory sticks or personal devices it must be encrypted. When taken off site in paper form (school trips) due care must be taken.

- Use of personal email accounts or [unencrypted] personal devices by governor or staff for official school business is not permitted.

9. Processing of Financial / Credit Card Data

The school complies with the requirements of the PCI Data Security Standard (PCI DSS). Staff who are required to process credit 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 Foundation Bursar. 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), may not be treated as legally sensitive but can have material impact on individuals and should be handled accordingly.

“It is in everyone's interests to get data protection right and to think carefully about data protection issues: this means handling all personal information with which you come into contact fairly, lawfully, securely and responsibly.

A good rule of thumb here is to ask yourself questions such as:

- Would I be happy if my own personal information were being used (for example, shared with a third party) in the way I am proposing? Would I expect it?

- Would I wish to stand by how I have recorded this information in an email or official record if the person concerned was able to see it? Please refer to e-mail protocol for guidance at Appendix 2.

- What would be the consequences of my losing or misdirecting this personal data?

Data protection law is therefore best seen not as oppressive red tape, or a reason not to do something necessary or important, but a code of useful and sensible checks and balances to improve how handle and record personal information and manage our relationships with people. This is an important part of the school’s culture and all its staff and representatives need to be mindful of it.”

Appendix 1

Storage & Retention of Records and Documents

Table of Suggested Retention Periods

Type of Record/Document	**Suggested [1] Retention Period**	**Person Responsible**
School Specific Records • Registration documents of School	Permanent (or until closure of the school)	Foundation Bursar
• Minutes of Governors' meetings	6 years from date of meeting	Clerk to the Governors
• Annual curriculum	From end of year: 3 years (or 1 year for other class records: eg marks / timetables / assignments)	Deputy Head (Academic)
Individual Pupil Records	***NB – this will generally be personal data***	
• Admissions: application forms, assessments, records of decisions	25 years from date of birth (or, if pupil not admitted, up to 12 months from that decision).	Admissions Registrars then Head's office
• Attendance Register	25 years from date of birth	Head's office
• Examination results (external or internal)	25 years from date of birth	Exams Officers
• Pupil file including: - Pupil reports - Pupil performance records - Pupil medical records	25 years from date of birth (subject to where relevant to safeguarding considerations: any material which may be relevant to potential claims should be kept for the lifetime of the pupil).	Head's office during school career then archives
• Special educational needs records (*to be risk assessed individually*)	35 years from date of birth (allowing for special extensions to statutory limitation period)	Head's office during school career then archives
• Counselling records	25 years from date of birth	School Counsellors
• General administrative documents	No longer than one year after pupil leaving school	At the discretion of the person who created the document
• See also reference to Child Protection Records in Safeguarding Section	[This may be 25 years from date of birth OR indefinitely.]	

Retained Information When Individual Pupil Records are deleted/shredded, the following data shall be recorded on a record card (i.e. hard copy) and retained indefinitely. • Full Name • Date of Birth • Date of Joining • Date of Leaving • Day or Boarding at time of leaving • Country of residence • Grades and board for external exams taken at this school • Note of destination if known • UCAS reference, if pre 1990 hard copy • **Dates pupil file shredded/deleted (paper file / MIS record)[5]** • Does a file exist elsewhere Yes/No? • If Yes – for S.E.N. or Safeguarding records? **Everything else to be destroyed**		
Safeguarding • Policies and procedures	Keep a permanent record of historic policies	Senior Deputy Head
• DBS disclosure certificates (if held)	No longer than 6 months from decision on recruitment, unless DBS specifically consulted – but a record of the checks being made must be kept, if not the certificate itself.	HR Administration Manager
• Accident / Incident reporting	Keep on record for as long as any living victim may bring a claim (NB civil claim limitation periods can be set aside in cases of abuse). Ideally, files to be reviewed from time to time if resources allow and a suitably qualified person is available. [2]	Head's office
• Child Protection files	If a referral has been made / social care have been involved or child has been subject of a multi-agency plan – indefinitely. If low level concerns, with no multi-agency act – apply applicable school low-level concerns policy rationale (this may be 25 years from date of birth OR indefinitely).	Senior Deputy Head

Corporate Records (where applicable) • Certificates of Incorporation	**eg *where schools have trading arms*** Permanent (or until dissolution of the company)	

• Minutes, Notes and Resolutions of Boards or Management Meetings	Minimum – 10 years	Foundation Accountant
• Shareholder resolutions	Minimum – 10 years	
• Register of Members/Shareholders	Permanent (minimum 10 years for ex members/shareholders)	
• Annual reports	Minimum – 6 years	

Accounting Records [3]		
• Accounting records (*normally taken to mean records which enable a company's accurate financial position to be ascertained & which give a true and fair view of the company's financial state*) [NB specific ambit to be advised by an accountancy expert]	Minimum – 3 years for private UK companies (except where still necessary for tax returns) Minimum – 6 years for UK charities (and public companies) from the end of the financial year in which the transaction took place Internationally: can be up to 20 years depending on local legal/accountancy requirements	Foundation Accountant
• Tax returns	Minimum – 6 years	
• VAT returns	Minimum – 6 years	
• Budget and internal financial reports	Minimum – 3 years	
Contracts and Agreements		
• Signed or final/concluded agreements (*plus any signed or final/concluded variations or amendments*)	Minimum – 7 years from completion of contractual obligations or term of agreement, whichever is the later	Foundation Bursar
• Deeds (or contracts under seal)	Minimum – 13 years from completion of contractual obligation or term of agreement	Foundation Bursar
Intellectual Property Records		
• Formal documents of title (trade mark or registered design certificates; patent or utility model certificates)	Permanent (in the case of any right which can be permanently extended, eg trade marks); otherwise expiry of right plus minimum of 7 years.	Foundation Bursar

• Assignments of intellectual property to or from the school	As above in relation to contracts (7 years) or, where applicable, deeds (13 years).	Foundation Bursar
• IP / IT agreements (including software licences and ancillary agreements eg maintenance; storage; development; coexistence agreements; consents)	Minimum – 7 years from completion of contractual obligation concerned or term of agreement	Director of IT
Employee / Personnel Records	***NB this will contain personal data***	
• Single Central Record of employees	Keep a permanent record of all mandatory checks that have been undertaken (but not DBS certificate itself: 6 months as above)	Foundation Bursar
• Contracts of employment	7 years from effective date of end of contract	Foundation Bursar
• Employee appraisals or reviews	Duration of employment plus minimum of 7 years	Foundation Bursar
• Staff personnel file	As above, but do not delete any information which may be relevant to historic safeguarding claims	Foundation Bursar
• Payroll, salary, maternity pay records	Minimum – 6 years	Foundation Accountant
• Pension or other benefit schedule records	Possibly permanent, depending on nature of scheme	Foundation Accountant
• Job application and interview/rejection records (unsuccessful applicants)	Minimum 3 months but no more than 1 year	Foundation Bursar
• Immigration records	Minimum – 4 years	Foundation Bursar
• Health records relating to employees	7 years from end of contract of employment	Foundation Bursar
Insurance Records		
• Insurance policies (will vary – private, public, professional indemnity)	Duration of policy (or as required by policy) plus a period for any run-off arrangement and coverage of insured risks: ideally, until it is possible to calculate that no living person could make a claim.	Foundation Accountant
• Correspondence related to claims/ renewals/ notification re: insurance	Minimum – 7 years	Foundation Accountant

Environmental, Health & Data • Maintenance logs	10 years from date of last entry	
• Accidents to children [4]	25 years from birth (longer for safeguarding)	
• Accident at work records (staff) [4]	Minimum – 4 years from date of accident, but review case-by-case where possible	Foundation Bursar
• Staff use of hazardous substances [4]	Minimum – 7 years from end of date of use	
• Risk assessments (carried out in respect of above) [4]	7 years from completion of relevant project, incident, event or activity.	
• Data protection records documenting processing activity, data breaches	No limit: as long as up-to-date and relevant (as long as no personal data held)	Foundation Bursar

Footnotes:

1. General basis of suggestion:

   Some of these periods will be mandatory legal requirements (eg under the Companies Act 2006 or the Charities Act 2011), but in the majority of cases these decisions are up to the institution concerned. The suggestions will therefore be based on practical considerations for retention such as limitation periods for legal claims, and guidance from Courts, weighed against whether there is a reasonable argument in respect of data protection.

2. The High Court has found that a retention period of 35 years was within the bracket of legitimate approaches. It also found that it would be disproportionate for most organisations to conduct regular reviews, but at the time of writing the ICO (Information Commissioner's Office) still expects to see a responsible assessment policy (eg every 6 years) in place.

3. Retention period for tax purposes should <u>always</u> be made by reference to specific legal or accountancy advice.

4. Be aware that latent injuries can take years to manifest, and the limitation period for claims reflects this: so keep a note of all procedures as they were at the time, and keep a record that they were followed. Also keep the relevant insurance documents.

5. The requirements of GDPR prevent personal data being kept for longer than is necessary for the purpose for which it was collected. However, they equally govern its premature destruction. We need to be able to clearly demonstrate that records were destroyed in accordance with the published policy.

6. **Clarification as to what Constitutes Controlled Data**
   We need to store all personal data securely, but we only need to control retention/destruction for the original record. So, for example, if a report of pupil medical notes is produced for an educational visit leader, that is a copy of the original records. It needs to be kept securely but we don't need to refer to any retention periods or keep a log regarding its disposal. It should be shredded as soon as the trip is over. Likewise, a printed copy of a pupil's school report, these are all on SIMS/PASS and paper copies may be shredded at any time without reference to retention rules.

Appendix 2

Haberdashers' Monmouth Schools

Email Protocol

Please consider the following guidelines when using school email.

- Consider carefully the timings of sending an email and especially so during evenings and weekends. Of course for many colleagues these times might be when they can read and send emails but expectation of sending and receiving should be during normal working hours. Do try and reply punctually (within 24 hours) to parents even if it is only a holding response

- Target recipients carefully and think twice before hitting 'Reply All'

- Distinguish between the main recipient who needs to take action or respond, and those who are included for information only. Consider whether email is sufficiently confidential: emails are very easy to forward to a much larger audience

- Consider what text has gone before when forwarding emails

- Carefully monitor tone of emails before sending. If you receive a negative email don't aggravate matters by sending a hasty, misjudged response. Leave your reply as a draft for a time before reviewing and sending. Alternatively phone the sender and arrange to discuss the issues on the phone or, ideally, face-face.

- Take care with spelling, punctuation and grammar and consider how you address the recipient and your type of sign off

- Avoid capitals since these can be construed as shouting

- Switch off the option to request 'delivery or read' receipts; only use it if it is absolutely essential for emails to specific people

- Do not send large attachments to many people. Put the document on appropriate school system and send colleagues the link

- Try to avoid school email groups for private business i.e. sponsorship requests, items for sale etc

- It is acceptable to post 'out of office' emails during school holidays and a response along the lines of the following will suffice: *'I am on holiday and will reply to your email when school reopens. If you have a pressing concern please contact Reception for advice. Thank you'*

- Please be aware of the key points raised in our Data Protection policy. No email is confidential as a result of subject access requests so only write what you would want to be attributable to you.

JMOC
January 2020