The Mall School

# DATA PROTECTION POLICY

## 1. Background

Data protection is an important legal compliance issue for the School. During the course of the School's activities we collect, store and process 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 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 – 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 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.

## 3. 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 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.

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 School

The School has appointed the Bursar 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 the General Data Protection Regulation (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 Lead.

## 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:

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.

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 for 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.

## 6. Lawful grounds for data processing

The School's lawful grounds are set out in its Privacy Policy.

## 7. Main 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 they are dissatisfied with how it is recorded. This applies to how staff record the personal data of others – in particular colleagues, pupils and their parents – in a way that is accurate, 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.

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 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:

- Safeguarding
- ICT
- Email

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

If you are concerned that there has been a data breach you must inform the Bursar immediately. If the data breach is likely to result in high risk to an individual's rights and freedoms he will notify the Information Commissioner's Office (ICO) and the individual concerned, within 72 hours. The School will keep a record of any personal data breaches regardless of whether we need to notify the ICO. Failure to report a breach of personal data may be considered as a serious disciplinary matter.

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 affects daily processes: filing and sending correspondence, notably hard copy documents. Data handlers should always consider what their most assured and secure means of delivery is, and what the consequences would be of loss or unauthorised access.

We expect all those with management and leadership responsibilities to be champions of these principles and to oversee the swift reporting of any concerns about how personal information is used by the School to the Bursar and to identity the need for, and implement, regular staff training. Staff must attend any training we the School requires them to.

8. Rights of Individuals

In addition to the School's responsibilities when processing personal data, individuals have certain specific rights, including access to their personal data held by a data controller. 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 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;
- 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 ones 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 Bursar as soon as possible.

## 9 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. As such, 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 the Headmaster or Bursar. The School will ensure that all personal information is held securely and is not accessible to unauthorised persons. There will be occasions when staff need to take home, or elsewhere, data related to pupils or the School. All staff will be made aware of their responsibility to prevent unauthorised access to any personal information they hold. Where a worker is permitted to take data offsite it will need to be encrypted. Use of personal email accounts or unencrypted personal devices for official School business is not permitted.

Any confidential information on pupils, parents or staff which is no longer required (including draft copies of reports) must be disposed of by shredding.

A breach of this policy might be considered a disciplinary matter.

## 10. CCTV

The Mall operates a CCTV system on the main site which covers the pedestrian and vehicular entrances to the School. The system and the images produced by it are overseen by the Bursar who is responsible for how the system is used and for notifying the Information Commissioner about the CCTV system and its purpose. The Mall has considered the need for using CCTV and has decided it is required for the prevention and detection of crime and for protecting the safety of pupils, parents and staff. The School, having fully considered the privacy rights of individuals, believes that data captured for these purposes are all in its legitimate interests. It will not be used for commercial or any other purposes.

## 11. Processing of Financial/Credit Card Data

The School complies with the requirements of the PCI Data Security Standard. Staff who are required to process credit card data must ensure that they are aware of and comply with the most up to date requirements. If you are unsure in this regard, please seek further guidance from the 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.

## 12. Retention

Under the Freedom of Information Act 2000, schools are required to maintain a retention schedule listing the records which the school creates in the course of its business. Staff will follow the guidance provided by the Information and Records Management Society regarding retention periods and correct method of disposal for records held by the School. The Retention Schedule (Appendix 1) lays down the length of time which the record needs to be retained and the action which should be taken when it is of no further administrative use.

Members of staff are expected to manage their current record keeping systems using the Retention Schedule and to take account of the different kinds of retention periods when they are

creating new record keeping systems. The Retention Schedule refers to all information, regardless of the media in which they are stored.

## 13. Summary

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?
- 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.

## 14. Enforcement

If an individual believes that the School has not complied with this Policy or acted otherwise than in accordance with the Data Protection Act, they should utilise the School whistleblowing procedure and should also notify the Bursar.

The Mall School
Revised Summer 2022
(Review Summer 2025)

**Appendix 1**
**DATA PROTECTION POLICY**

**RETENTION SCHEDULE**

| **Type of Record/Document** | **Retention Period** |
|---|---|
| SCHOOL-SPECIFIC RECORDS<br><br>Registration documents of School<br>Attendance Register<br>Minutes of Governors' meetings<br>Annual curriculum | <br><br>Permanent (or until closure of the school)<br>6 years from last date of entry, then archive.<br>6 years from date of meeting<br>From end of year: 3 years (or 1 year for other class records: e.g. marks / timetables / assignments) |
| INDIVIDUAL PUPIL RECORDS<br><br>Admissions: application forms, assessments, records of decisions<br>Examination results (external or internal)<br>Pupil file including:<br>Pupil reports<br>Pupil performance records<br>Pupil medical records<br>Special educational needs records (to be risk assessed individually) | ***NB – this will generally be personal data***<br>25 years from date of birth (orup to 7 years from the pupil leaving). If unsuccessful: up to 1 year.<br>7 years from pupil leaving school<br>ALL: 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).<br>Date of birth plus up to 35 years (allowing for special extensions to statutory limitation period) |

| | |
|---|---|
| SAFEGUARDING | |
| Policies and procedures | Keep a permanent record of historic policies |
| 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. |
| 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. |
| Child Protection files | If a referral has been made / social care have been involved or child has been subject of a multi-agency plan; or there is a risk of future claims – indefinitely.<br><br>If low level concerns, with no multi-agency action, consider whether or not the child needs to be named in any record concerning an adult or if a copy should be kept on the child protection file. |
| CORPORATE RECORDS (where applicable) | |
| Certificates of Incorporation | Permanent (or until dissolution of the company) |
| Minutes, Notes and Resolutions of Boards or Management Meetings | Minimum – 10 years |
| Shareholder resolutions | Minimum – 10 years |
| Register of Members/ Shareholders | Permanent (minimum 10 years for ex-members/shareholders) |
| Annual reports | Minimum – 6 years |

| | |
|---|---|
| ACCOUNTING RECORDS | |
| 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) | Minimum – 3 years for private UK companies (except where still necessary for tax returns)<br>Minimum – 6 years for UK charities (and public companies) from the end of the financial year in which the transaction took place<br>Internationally: can be up to 20 years depending on local legal/accountancy requirements |
| 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 |
| Deeds (or contracts under seal) | Minimum – 13 years from completion of contractual obligation or term of agreement |
| 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. |
| Assignments of intellectual property to or from the school | As above in relation to contracts (7 years) or, where applicable, deeds (13 years). |
| IP / IT agreements (including software licences and ancillary agreements e.g. maintenance; storage; development; coexistence agreements; consents) | Minimum – 7 years from completion of contractual obligation concerned or term of agreement |
| EMPLOYEE / PERSONNEL RECORDS | **NB this will contain personal data** |
| Single Central Record of employees | Keep a permanent record that mandatory checks have been undertaken (but do not keep DBS certificate information itself: 6 months as above) |
| Contracts of employment | 7 years from effective date of end of contract |
| Employee appraisals or reviews | Duration of employment plus minimum of 7 years |
| Staff personnel file | As above, but do not delete any information |

| | |
|---|---|
| | which may be relevant to historic safeguarding claims. |
| Payroll, salary, maternity pay records | Minimum – 6 years |
| Pension or other benefit schedule records | Possibly permanent, depending on nature of scheme |
| Job application and interview/rejection records (unsuccessful applicants) | Minimum 3 months but no more than 1 year |
| Immigration records | Minimum – 4 years |
| Health records relating to employees | 7 years from end of contract of employment |
| Low level concerns about adults | Regular review recommended to justify longer-term retention as part of safeguarding files. |
| 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. |
| Correspondence related to claims/ renewals/ notification re: insurance | Minimum – 7 years |
| ENVIRONMENTAL, HEALTH & DATA | |
| Maintenance logs | 10 years from date of last entry |
| Accidents to children | 25 years from birth (longer for safeguarding) |
| Accident at work records (staff) | Minimum – 4 years from date of accident, but review case-by-case where possible |
| Staff use of hazardous substances | Minimum – 7 years from end of date of use |
| Risk assessments (carried out in respect of above) | 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) |