MALVERN ST JAMES
Girls' School

# Data Protection Policy

This policy is the responsibility of the Director of Operations and Compliance, to review and update annually.

## Scope

The School aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors, Old Girls' Association members, MSJ Community members and other individuals is collected, stored and processed in accordance with the UK General Data Protection Regulation (UK GDPR), which has consolidated and amended the Data Protection Act 2018 (DPA 2018) and the General Data Protection Regulations.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

## Legislation and guidance

This policy meets the requirements of the UK GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and the ICO's code of practice for subject access requests.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

## 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, Old Girls' Association members and MSJ Community members, 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. Accidental breaches 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 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 personal data held by the School, 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.

**Definitions**

| Term | Definition |
|---|---|
| **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. |
| **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. |
| **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. |
| **Data subject** | The identified or identifiable individual whose personal data is held or processed. |
| **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. |
| **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. |

**The Data Controller**

Our School processes personal data relating to parents, pupils, staff, governors, Old Girls' Association and MSJ Community members, visitors and others, and therefore is a data controller.

The School is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

**Roles and responsibilities**

This policy applies to **all staff** employed by our School, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

**Governing board**. The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

**Information Compliance officer**. The Information Compliance officer (ICO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

The School has appointed the Director of Operations and Compliance as the Information Compliance Officer, with responsibility for ensuring that all personal data is processed in compliance with this Policy and the principles of the UK 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 Information Compliance Officer.

**All staff.** Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the School of any changes to their personal data, such as a change of address
- Contacting the Information Compliance Officer in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside of the School
    - If there has been a suspected data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they want to share information with third parties

**Data protection principles**

The UK 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 UK 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.

**Collecting personal data**

**Lawfulness, fairness and transparency.** We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task in the public interest, and carry out its official functions
- The data needs to be processed for the legitimate interests of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/guardian when appropriate in the case of a pupil) has freely given clear consent

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the UK GDPR .

**Limitation, minimisation and accuracy**

The School will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's Retention Schedule, which is attached below.

**Sharing personal data**

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/guardian that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils and members of our Old Girls' Association and MSJ Community – for example, IT companies and mailing houses.

When doing this, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the UK, we will do so in accordance with data protection law.

**Subject access requests and other rights of individuals**

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests can be accepted in any form including verbally or via social media, however we will need to confirm identification prior to fulfilling the request. A request will be processed quicker if submitted in writing, either by letter, email or fax and including:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request, they must immediately forward it to the Director of Operations and Compliance as soon as possible.

**Children and subject access requests**

Personal data about a child belongs to that child, and not the child's parents or guardians. For a parent or guardian to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.
Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or guardians of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

**Responding to subject access requests**

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if, for example, it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

**Other data protection rights of the individual**

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area

- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine- readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the Information Compliance Officer. If staff receive such a request, they must immediately forward it to the Information Compliance Officer.

Whilst GDPR enshrines the "right to be forgotten", the School will sometimes have compelling reasons to refuse specific requests to amend, delete or stop processing the personal data of pupils: for example, a legal requirement, or where it falls within a legitimate interest identified in the School's Privacy Notice. All such requests will be considered on their own merits.

**Parental requests to see the educational record**

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request. However, as a Free School, there is no automatic parental right of access to the educational record in our setting. We will endeavor to meet the responsibilities of maintained schools when parents request their child's educational record.

It should be noted that (as per the School's Privacy Notice) the School is not required to disclose any pupil examination scripts (or other information consisting solely of pupil test answers), provide examination or other test marks ahead of any ordinary publication, nor share any confidential reference given by the School itself for the purposes of the education, training or employment of any individual.

**Data protection by design and default**

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified Information Compliance Officer, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law
- Completing privacy impact assessments where the School's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the Information Compliance Officer will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of this training
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our School and Information Compliance Officer and all information we are required to share about how we use and processtheir personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

**Data security and storage of records**

The School will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access. Walk-up print management is installed to avoid information being left on printers.
- Where personal information needs to be taken off site, it must be included in the Visit Pack and authorized by the Information Compliance Officer
- Passwords that are at least 8 characters long containing letters and numbers are used to access School software. Staff and pupils are reminded to change their passwords at regular intervals
- Use of personal email accounts for official School business by governors and staff is not permitted.
- Encryption software (Bitdefender) is used to protect all portable devices and removable media, such as laptops and USB devices
- MDM and MAM policies are in place to ensure all Staff, pupils or governors who access School information on their personal devices are protected.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected

**Retention and Disposal of records**

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the School's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

The School follows the advice set out by the Information and Records Management Society (IRMS) http://irms.org.uk/. We will always use the latest version of the toolkit http://irms.org.uk/page/SchoolsToolkit.

For ease of reference, the retention and disposal schedules are broken down into 5 sections:

- Governing Body
- School Management
- Pupil Administration
- Curriculum and Extra-Curricular Activities
- Central Government and Local Authority

**Personal data breaches**

The School will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being publised
- Safeguarding information being made available to an unauthorised person
- The theft of a School device containing non-encrypted personal data about pupils

**Training**

All staff and governors are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the School's processes make it necessary. Staff conduct UK GDPR training annually and this is recorded in Smartlog.

**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. 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.

**Appendix 1: Personal data breach procedure**

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Information Compliance Officer
- The Information Compliance Officer will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The Information Compliance Officer will make all reasonable efforts to contain and minimise the impact of the breach, assisted by the IT Manager and relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The Information Compliance Officer will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The Information Compliance Officer will work out whether the breach must be reported to the ICO. This must be judged on a case-by- case basis. To decide, the Information Compliance Officer will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned
- If it's likely that there will be a risk to people's rights and freedoms, the Information Compliance Officer must notify the ICO. The Information Compliance Officer will alert the Headmistress and Chair of Governors immediately.
- The Information Compliance will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored in the Data Breach log in the Operations MS Team.
- Where the ICO must be notified, the Information Compliance will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the Information Compliance Officer will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the Information Compliance Officer
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and

mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the Information Compliance Officer will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the Information Compliance Officer expects to have further information. The Information Compliance Officer will submit the remaining information as soon as possible
- The Information Compliance Officer will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the Information Compliance Officer will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the Information Compliance Officer
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The Information Compliance Officer will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The Information Compliance Officer will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
- The Information Compliance Officer will review what happened and how it can be stopped from happening again.

**Actions to minimise the impact of data breaches**

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

**Sensitive information being disclosed via email (including safeguarding records)**

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Other types of breach that you might want to consider could include:

- Details of named children being published on the school website – delete the information as soon as it is identified; check website for number of page hits.

- Non-anonymised pupil exam results or staff pay information being shared with governors – remind governors of statutory duty regarding data protection, ask for all copies to be returned and destroyed
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked – inform Police, DPO and ICO immediately. Attempt to recover the information.
- The school's cashless payment provider being hacked and parents' financial details stolen – Contact affected parties immediately, inform Police, DPO and ICO immediately
- Paper copies of pupil details being lost e.g. when on a school trip – Provide all trip leaders with lockable folder, inform DPO and ICO immediately.

**Appendix 2: Staff Responsibilities**

All staff and volunteers at MSJ have a responsibility to ensure data is protected. We will create a data safe environment by doing the following:

- Lock all computers when leaving the screen
- Following all school policies regarding photographs, mobile phones and social networking
- Only taking electronic information off-site using an encrypted memory stick
- Ensuring any school electronic devices have a secure password
- Not sending sensitive information via email – the school will consider using encrypted email if required
- Ensuring all bulk emails are sent using BCC to avoid sharing contact details
- Ensuring the school's internet filtering is used
- Ensuring any personal information is not freely available e.g. on display
- Ensuring any sensitive information is in a locked cupboard
- Ensuring we do not discuss sensitive information with people who do not need to know
- Signing any paper copies of information we take off site on the register in the school office, and signing it back in.
- Dispose of any redundant data securely
- Ensure all data we own is up to date and accurate
- Reporting any data breaches to the head teacher immediately
- Completing the data breach documentation as soon as possible afterwards
- Teach children about data protection and how to keep their data safe.

| | |
|---|---|
| **Authorised by** | Resolution of THE SCHOOL COUNCIL |
| **Signature** |  |
| **Date** | 5 December 2022 |

| | |
|---|---|
| **Effective date of the policy** | 5 December 2022 |
| **Review date** | Spring Term 2023 |
| **Circulation** | Members of School Council / teaching staff / all staff. (Parents & pupils on request) |