St Mary's School
CAMBRIDGE

Data Protection Policy

This policy is the responsibility of the Bursar and the Head of HR and Compliance.

Last review: March 26

Next review: March 28

Background

Data protection is an important legal compliance issue for St Mary's School ('the School'). During the course of the School's activities it collects, stores and processes personal and sensitive data about staff, pupils (including EYFS), their parents, volunteers, 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.

General Data Protection Regulation (**GDPR**) was implemented in 2018. GDPR is an EU Regulation that is directly effective in the UK and a new 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 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, will typically investigate individuals' complaints routinely and without cost, and has various powers to take action for breaches of the law.

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 School 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.

Data subject - a natural person or individual whose personal data is processed by a data controller or processor. A data subject can be identified by various identifiers, such as name, ID number, location data, or other factors related to their identity.

Virtually any information about someone is likely to be personal data and examples are listed below:

- contact details and other personal information held about pupils, parents, prospective parents and staff and their families;
- information about a child protection incident;
- emails expressing opinion or intention in relation to a person;
- a record about disciplinary action taken against or an investigation into a member of staff;
- photographs, video images or voice recordings of pupils or staff;
- financial records;
- records of staff sickness absence or leave.

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.

Those who handle personal data as employees or governors of the School are obliged to comply with this policy when doing so. For employees, depending on the nature, 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.

Person responsible for Data Protection at the School

The School has appointed the Compliance Manager 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 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 Compliance Manager or Bursar.

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;
6. processed in a manner that ensures appropriate security of the personal data.

The GDPR's 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;
- 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.

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.

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 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.

Data handling and individual responsibilities

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:

The IT Acceptable Use Policy, Online Safety Policy, Safeguarding and Child Protection Policy, Taking, Storing and Using Images of Children Policy, Social Media policy, Bring Your Own Device to Work Policy and the data retention guidelines. These documents can be found on the policies page of the website and on the St Mary's Cloud – All Staff – Policies tile.

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.

You may have access to personal data of other members of staff, pupils, parents, suppliers, alumnae, contractors, and governors of the School in the course of your employment or engagement.

If you have access to personal data, you must:

- only access the personal data that you have authority to access, and only for authorised purposes;
- only allow others to access personal data if they have appropriate authorisation;
- keep personal data secure by complying to rules on access to premises, computer access, password protection, secure file storage and retention and destruction;
- not remove personal data, or devices containing personal data (or which can be used to access it), from the School's premises unless appropriate security measures are in place (such as encryption or password protection);
- not store personal data on local drives or on personal devices;
- not use personal email accounts or unencrypted personal devices for official School business and you must act in accordance with our Bring Your Own Device to Work Policy (BYOD);
- not transfer data outside the EU without authorisation from IT and the Compliance Manager.

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 IT Director and the Head of HR and Compliance. 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 The Principles 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. 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.

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 Bursar and to identify the need for (and implement) regular staff training. Staff must attend any training we require them to.

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 Compliance Manager 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.

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;
- 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 Compliance Manager as soon as possible.

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. See Data Handling and Individual Responsibilities above.

Sharing Personal Data and information security

The general position is that personal data should only be shared in a "need to know" basis. This will not prevent sharing where doing so is lawful, fair, reasonable and proportionate and done in accordance with this Policy and the sharing guidelines. Staff should speak to the Compliance Manager if in doubt, or if staff are being asked to share personal data in a new way. Before sharing personal data, staff should:

- refer to the Data Sharing Checklist, Code, 365 sharing guide and Information Sharing Advice – safeguarding in the St Mary's cloud in the data protection tile;
- make sure they are allowed to share it;
- ensure adequate security;
- ensure that any emails which contain sensitive personal data are encrypted;
- if asked to disclose information to the Police speak to the Compliance Manager and ensure the request is made in writing;
- if asked to disclose personal data to a contractor or to an individual where they are unsure of identity (e.g. if a request has come from a parent using a different or non- registered email address) they should check with their line manager and the Compliance Manager.

Information security is important, and all staff should seek to ensure that security breaches do not occur. Examples in a school environment could be leaving a mobile phone in a public place which is not password protected, sending personal data or special category personal data to the wrong recipient, disposing of confidential documents without shredding them first or accidentally uploading confidential information to the web. Staff must do all they can to ensure that personal data is not lost or damaged or accessed or used without proper authority.

Staff should:

- be careful when sending correspondence containing personal data and/or special category data. Staff should check email addresses and if in doubt send a 'test' email. Extreme care must be taken when attaching files to emails;
- be careful when sharing documents in the St Mary's cloud – see the 365 data sharing guidelines in all staff, data protection;

- do not use or leave computers, devices or papers where there is a significant risk that they may be viewed or taken by unauthorised persons;
- be vigilant of the risks of others viewing confidential documents. Paper documents should be locked away when not in use and carried in envelopes/folders;
- use bcc (blind carbon copy) where appropriate;
- lock their computers when not in use;
- keep passwords secure;
- use encryption where handling personal or confidential data;
- refer to the BYOD Policy regarding use of personal devices.

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 Bursar/Finance Manager. 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.

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 we 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.