Data Protection Policy

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

Scope

This Policy is not to be confused with the School's Privacy Notice, which is a General Data Protection Regulation (GDPR) requirement (and must generally be provided directly to data subjects). This Policy is not aimed at external audiences to tell them how their personal data is used, but primarily at staff. It determines how, as a matter of good practice and policy, any personal data controlled and processed by the School – covering parents, pupils, and colleagues (past, present or prospective), should be handled by staff. The Policy does not apply to teaching resources unless for some reason they contain identifiable personal details of pupils.

Background

Data protection is an important legal compliance issue for Malvern St James School ['The School']. 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 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.

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 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 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**) who is responsible for enforcing data protection law, will typically look into 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 of pupils' personal information. As a data controller, we are responsible for safeguarding the use of personal data.
- **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/Data Incident** – 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. **Important Note**: Personal information created in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings) is still personal data and regulated by data protection laws, including the GDPR. Note also that it includes expressions of opinion about the individual or any indication of someone'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.

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. 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 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.

School Lead for Data Protection

The School has appointed the Director of Operations & 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 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.

Data Protection 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 '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; 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, how and when data protection consents were collected from individuals, how breaches were dealt with, 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 and can automatically expire with time) it is generally considered preferable 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 Controller. It can be challenged by data subjects and also means the Controller 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 Policy, as GDPR requires.

Other lawful grounds include:

- **compliance with a legal obligation**, including in connection with employment and diversity;
- **contractual necessity**, e.g. to perform a contract with staff or parents;
- 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.

Responsibilities of <u>ALL</u> 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 *their own* personal data is inaccurate or untrue or if they are dissatisfied with how it is recorded. This applies to how staff record their own data, and the personal data of others – in particular colleagues, pupils and their 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.

Data handling

All staff must 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. 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 related policies:

- Acceptable Use of IT and the Internet Policy
- Accessibility Policy
- Anti-bullying Policy
- Safeguarding Policy
- E-safety Policy
- School Mini bus Policy
- Educational Visits Policy
- CCTV Policy
- Critical Incident Policy
- Anti-bullying Policy
- Pastoral Care 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. The School must report certain types of personal data breach (those which risk an impact to individuals) to the ICO within 72 hours of the incident being discovered.

The School must also notify individuals affected if the breach is likely to result in a "high risk" to their rights and freedoms. The School must keep a record of any personal data breaches or 'data incidents', regardless of whether we need to notify the ICO. If staff become aware of a personal data breach, they must notify the Director of Operations & Compliance immediately. If staff are in any doubt as to whether or not to report an issue, 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 staff member's contract.

Care and data security

More generally, the School requires all staff to remain conscious of the data protection principles above, to comply with those principles whenever they process personal information and to attend any training required.

Data security is not simply an online or digital issue but one that effects daily processes: filing and sending correspondence, notably hard copy documents. When sending documents or data, staff should always assess what they consider the most secure means of delivery is, and the consequences

of loss or unauthorised access.

The School 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 Director of Operations & Compliance and to identity the need for (and implement) regular staff training.

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 Director of Operations & Compliance 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 (i.e. tailored products aimed at an individual or Emails/texts sent to parents to inform of school events, closures etc. are not a form of direct marketing); and
- withdraw their consent where we are relying on it for processing their personal data – the right to be forgotten (anyone who refuses consent or withdraws it at any stage must be removed from our records).

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.

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.

If staff receive a request from an individual who is purporting to exercise one or more of their data protection rights, you must tell the Director of Operations & Compliance as soon as possible.

Data Security: online and digital

Taking data off site. The School has a responsibility to 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 paper (eg reports or mark books) or electronic form, without the prior consent of the Headmistress, Deputy Head or Director of Operations & Compliance. The School permits the use of remote access working; this needs to be set up through the network manager.

Email. Under no circumstances should pupil reports, staff reports or personal data be emailed to personal i.e. non-school, email accounts or cloud storage. The use of School email accounts on personal devices is only permitted with PIN/password protection and the ability to remotely wipe the device should it be lost or stolen. (Note that remote erasure is difficult on desk top PCs so School data should not be stored on such machines.)

Processing of Financial or Credit Card Data. The School complies with the requirements of the Payment Card Industry 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 Director of Operations & Compliance. 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 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."

Authorised by	Resolution of THE SCHOOL COUNCIL
Signature	
Date	October 2019

Effective date of the policy	October 2019
Review date	August 2020
Circulation	Members of School Council / teaching staff / all staff. (Parents & pupils on request)