DATA PROTECTION POLICY

1. Introduction

Data protection is an important legal compliance issue for the Oratory 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 Notices). 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 "UK 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 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** – a person or body that determines the purpose and means of the processing of personal data, and who is legally responsible for how it is used. For example, the School (including by its governors) is a controller. An independent contractor who makes their own such decisions is also, separately, likely to be a data controller.

- **Data processor** – an organisation that processes personal data on behalf of a data controller, for example a payroll or IT provider or other supplier of services with whom personal data may be shared but who is not authorised to make any decisions about how it is used.

- **Personal data breach** – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

- **Personal information (or 'personal data'):** any information relating to a living individual (a data subject) by which that individual may be identified by the controller. That is not simply a name but any form of identifier, digital or contextual, including unique ID numbers, initials, job titles or nicknames. Note

that personal information will be created almost constantly in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings). The definition includes expressions of opinion about the individual or any indication of the School's, or any person's, intentions towards that individual.

- **Processing** – virtually anything done with personal information, including obtaining or collecting it, structuring it, analysing it, storing it, sharing it internally or with third parties (including making it available to be viewed electronically or otherwise), altering it or deleting it.

- **Special categories of personal data –** data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health and medical conditions, sex life or sexual orientation, genetic or biometric data used to identify an individual. There are also separate rules for the processing of personal data relating to criminal convictions and offences.

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 as 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 "processors" on the School's behalf (in which case they will be subject to binding contractual terms) or as 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 – 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.

Volunteers and contractors may, depending on the nature of their role, act either under the School's direction or as independent data controllers. In all cases they must comply with applicable data protection law and this policy.

Data Protection at the School

The Data Protection Officer is responsible for overseeing data protection within the School
so if you do have any questions in this regard, please do contact them on the information
below: -

Data Protection Officer: Judicium Consulting Limited
Address: 72 Cannon Street, London, EC4N 6AE

4. The Principles

The UK GDPR sets out six principles relating to the processing of personal data which must be adhered to by controllers (and 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 ("DPIA")); and
- generally having an 'audit trail' vis-à-vis data protection and privacy matters, including for example when and how our Privacy Notice(s) were updated; when staff training was undertaken; how and when any data protection consents were collected from individuals; how personal data breaches were dealt with, whether or not reported (and to whom), etc.

5. Lawful grounds for data processing

Under the UK GDPR there are several different lawful grounds for processing personal data. One of these is consent. However, given the relatively high bar of what constitutes consent under the UK 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 Notices, as the UK GDPR requires.

Other lawful grounds include:

- compliance with a legal obligation, including in connection with employment, engagement of services and diversity;
- contractual necessity, e.g. to perform a contract with staff or parents, or the engagement of contractors;
- a narrower set of grounds for processing special categories of personal data (such as health information), which includes explicit consent, emergencies, and specific public interest grounds.

6. Headline responsibilities of all staff

Record-keeping

It is important that personal data held by the School is accurate, fair and adequate. Staff are required to inform the School if they believe that *any* personal data is inaccurate or untrue or if you are dissatisfied with how it is recorded. This applies to how staff record their own data, and the personal data of others – in particular colleagues, pupils and their parents – in a way that is professional and appropriate.

Staff should be aware of the rights set out below, whereby any individuals about whom they record information on School business (notably in emails and notes) digitally or in hard copy files may have the right to see that information. This absolutely must not discourage staff from making necessary and sometimes difficult records of incidents or conversations involving colleagues or pupils and parents, 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 Employment 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 and Child Protection**
- **Social Media**
- **IT Acceptable Use Policy**
- **Information Security Policy**
- **Taking, Storing and Using Images of Children Policy**
- **Staff Code of Conduct**
- **Health and Safety Policy**
- **School Terms and Conditions**
- **CCTV policy**
- **Biometrics 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 obligations contained in the UK GDPR is on reporting personal data breaches. Controllers must report certain types of personal data breach (those which risk an impact to individuals) to the ICO within 72 hours.

In addition, 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 Bursar and/or the Data Protection Officer immediately. If staff are in any doubt as to whether to report something internally, it is always best to do so. A personal data breach may be serious, or it may be minor; and it may involve fault or not; but the School always needs to know about them to make a decision.

As stated above, the School may not need to treat the incident itself as a disciplinary matter – but a failure to report could result in significant exposure for the School, and for those affected, and could be a serious disciplinary matter whether under this policy or the applicable staff member's contract.

Care and data security

More generally, we require all School staff (and expect all our contractors) to remain mindful of the data protection principles (see section 5 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 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 / 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 identity the need for (and implement) regular staff training. Staff must attend any training we require them to.

Use of third party platforms / suppliers

As noted above, where a third party is processing personal data on the School's behalf it is likely to be a data 'processor', and this engagement must be subject to appropriate due diligence and contractual arrangements (as required by the UK GDPR). It may also be necessary to complete a DPIA before proceeding – particularly if the platform or software involves any sort of novel or high risk form of processing (including any use of artificial intelligence ("AI") technology). Any request to engage a third party supplier should be referred to the Bursar in the first instance, and at as early a stage as possible.

7. Rights of Individuals

In addition to the School's responsibilities when processing personal data, individuals have certain specific rights, perhaps most significantly that of access to their personal data held by a 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 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; and
- 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; and
- withdraw one's consent where we are relying on it for processing their personal data (without affecting the lawfulness of processing carried out prior to that point in reliance on consent, or of any processing carried out on some other legal basis other than consent).

In any event, however, if you receive a request from an individual who is purporting to exercise one or more of their data protection rights, you must tell the Bursar as soon as possible.

8. Data Security: online and digital

The School must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

- No member of staff is permitted to remove personal data whether in paper or electronic form and wherever stored, without prior consent of the Head or Bursar
- No member of staff should provide personal data of pupils or parents to third parties, including a volunteer or contractor, unless there is a lawful reason to do so.
- Where a worker is permitted to take data offsite on memory sticks or personal devices it will need to be encrypted.
- Use of personal email accounts or unencrypted personal devices by governors or staff for official School business is not permitted.

***Please refer to Appendix 1 of this Policy for Data Protection Tips.**

9. Processing of Financial / Credit Card Data

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

POLICY STATEMENT

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 to handle and record personal information and manage our relationships with people. This is an important part of the School's culture and all its staff and representatives need to be mindful of it.

Appendix 1

Top Tips for Data Protection

Background

80% of data breaches involve staff within an organisation (figure from the Information Commissioner's Office) and breaches, for the most part, are unintentional. Therefore, everyone dealing with Personal Data needs to have a basic understanding of the Data Protection Law. The School collects a variety of personal data on students, parents, alumni, contractors, staff, volunteers, business contacts etc for legitimate business reasons in connection with the running of the School. It is vital that all this information is kept securely, is regularly reviewed and disposed of when no longer required.

Top Data Protection Tips:

1. Read and follow the School's Data Protection Policy

2. Make sure all new staff within your department are aware of the School's policy and any departmental procedures on data protection.

3. Use strong passwords on all devices and two step-authentication wherever possible. Ensure that any device you access school personal data on (mobiles for instance) are password protected.

4. It is preferable not to but if you do use portable memory devices, ensure these are encrypted (memory sticks, hard drives etc - the IT department can advise on this).

5. Only keep information as long as necessary - conduct periodic reviews (at least yearly) of personal systems (paper and electronic) and delete personal data that is no longer required.

6. Remember that most data breaches are unintentional - double check who you are sending information to, don't leave computers unattended and unlocked and make sure you shred confidential information when it is no longer required.

7. Before sharing any personal information (this includes photos), check the school has the relevant permission to do so.

8. Use the One Drive and Microsoft Teams where possible and ensure the correct sharing permissions' are enabled. If these are sent in error, they can be wiped to limit access to the information.

9. If in any doubt about any personal data issue, contact the School's Data Protection Officer.

Further Information:

Tips on keeping information secure:

- Keep passwords secure – change these regularly and do not share or give other people your password. Use two step authentication.
- Always lock / log off computers when away from your desk
- Dispose of confidential paper waste securely by shredding
- Prevent virus attacks by taking care when opening emails and attachments or visiting new websites
- Hard copy personal information should be stored securely when it is not being used (lockable cabinets/drawers etc).
- Be careful when discussing individuals that you are not in earshot of anyone who does not need access to that information
- Position computer screens away from windows and walkways to prevent accidental disclosures of personal information
- Encrypt personal information that is being taken or sent outside the school or office.
- Do not, unless absolutely necessary, download personal data to a non-school device.

Tips on keeping only relevant information:

- Collect only the personal information required
- Explain new or changed business purposes to parents, pupils, employees and others, and obtain consent or provide an opt-out or opt-in where appropriate.
- Update records promptly – for example, changes of address, phone numbers.

● Delete personal information the School no longer requires. If in doubt, please check
whether the information should be retained. In the case of safeguarding information,
this should always be passed to the Designated Safeguarding Lead for him to decide whether or not the information should be retained. Please make reference to
the School's Document Retention Guidelines for the School.

● Be aware that there may be people who will try and trick staff into giving out personal information.

● Carry out identity checks before giving out personal information to anyone in person,
by writing or over the phone.

Handling requests from individuals for their personal information (subject access requests)

● People have a right to have a copy of the personal information the School holds

● Any requests for Personal Data should be forwarded to the School's Data Protection
Officer.