THE GRANVILLE SCHOOL

Data Protection Policy

Background

Data protection is an important legal compliance issue for The Granville 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 trustees/directors/governors in how they handle data. It is therefore an area where all staff have a part to play in ensuring we comply with and are mindful of our legal obligations, whether that personal data handling is sensitive or routine.

UK data protection law consists primarily of the UK version of the General Data Protection Regulation (the GDPR) and the Data Protection Act 2018 (DPA 2018). The DPA 2018 includes specific provisions of relevance to independent schools: in particular, in the context of our safeguarding obligations, and regarding the right of access to personal data.

Data protection law has in recent years strengthened the rights of individuals and placed tougher compliance obligations on organisations including schools that handle personal information. The Information Commissioner's Office (**ICO**) is responsible for enforcing data protection law and will typically look into individuals' complaints routinely and without cost, and has various powers to take action for breaches of the law.

Introduction

1 **Application:** This Policy is aimed at Staff including temporary staff, agency workers and volunteers. It also applies to Governors and contractors. It explains the School's general approach to data protection, and provides practical guidance which will help to ensure that the School complies with the **General Data Protection Regulations (GDPR)**

2 **Compliance:** Compliance with this policy will help the School to meet its obligations under the Regulations but it does not commit the School to a higher standard than is required by the Regulations. In some circumstances, e.g. situations involving safeguarding concerns strict compliance with the Regulations will be subsidiary to other considerations.

3 **Responsibility:** As the Data Controller, the School is responsible for complying with the Regulations. The Governing Body has delegated day to day responsibility for compliance with the Regulations to the Bursar / Director of Finance, Resources & Operations[1]. All staff are responsible for complying with this policy.

4 **Information security is the most important aspect of data protection compliance.** Most of the fines under the Regulations relate to security breaches such as leaving an unencrypted memory stick in a public place, sending sensitive documents to the wrong email recipient, disposing of confidential documents without shredding them first or accidentally uploading confidential information to the web. Further information can be found below.

Definitions

1 **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 Granville School (including by its trustees/directors/governors) is a controller. An independent contractor who makes their own such decisions is also, separately, likely to be a data controller.

2 **Data processor** – an organisation that processes personal data on behalf of The Granville School, for example our 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.

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

4 **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.

5 **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.

6 **Special categories of personal data (sensitive 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/trustees/directors 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 breach of discipline as per the School's disciplinary policy.

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 Granville

The School has appointed the Bursar / Director of Finance, Resource & Operations[1] as the Privacy & Data Protection Lead (PDPL) who will endeavour to ensure that all personal data is processed in compliance with this Policy and the principles of 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 Privacy & Data Protection Lead.

The Principles

The GDPR sets out six principles relating to the processing of personal data which must be adhered to by data controllers (and data processors). These require that personal data must be:

1. Processed **lawfully, fairly** and in a **transparent** manner;
2. Collected for **specific and explicit purposes** and only for the purposes it was collected for;
3. **Relevant** and **limited** to what is necessary for the purposes it is processed;
4. **Accurate** and kept **up to date**;
5. **Kept for no longer than is necessary** for the purposes for which it is processed; and
6. Processed in a manner that ensures **appropriate security** of the personal data.

The GDPR's broader 'accountability' principle also requires that The Granville 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.

Lawful grounds for data processing

1 The School shall only process Personal Data for specific and legitimate purposes. These are:

1.1 safeguarding and promoting the welfare of children;

1.2 ensuring that the School provides a safe and secure environment;

1.3 providing pastoral care;

1.4 providing education and learning for children;

1.5 providing additional activities for children and parents (for example activity clubs) ;

1.6 protecting and promoting the School's interests and objectives - this could include fundraising;

1.7 for personnel, administrative and management purposes, for example, to pay staff and to monitor their performance; and

1.8 to fulfil the School's contractual and other legal obligations.

2 School staff must not process Personal Data for any other purpose without the PDPL's permission.

3 **No incompatible purpose:** Staff should seek advice from the PDPL before using Personal Data for a purpose which is different from that for which it was originally acquired. If information has been obtained in confidence for one purpose, it shall not be used for any other purpose without the Bursar's permission.

4 **Necessary, sufficient information:** The School shall not hold unnecessary Personal Data, but shall hold sufficient information for the purpose for which it is required. The School shall record that information accurately and shall take reasonable steps to keep it up to date. This includes an individual's contact and medical details.

5 **Outside the EEA:** The School shall not transfer Personal Data outside the European Economic Area (**EEA**) without the Data Subject's permission unless it is satisfied that the Data Subject's rights under the Regulations will be adequately protected and the transfer has been approved by the Bursar. This applies even if the transfer is to a pupil's parents or guardians living outside the EEA.

6 **Fair:** When the School acquires personal information that will be kept as Personal Data, the School shall be fair to the Data Subject and fair to whoever provides the information (if that is someone else).

7 **Retaining Personal Data:** Staff shall only keep Personal Data for as long as is reasonably necessary, and in accordance with the Information and Records Retention and Security Policy, but staff should not delete records containing Personal Data without authorisation. Staff

should consult with the PDPL for guidance about how long to retain different categories of Personal Data.

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 recording necessary and sometimes difficult records of incidents or conversations involving colleagues or pupils, in accordance with the School's other policies, and grounds may sometimes exist to withhold these from such requests. However, the starting position for staff is to **record every document or email in a form they would be prepared to stand by should the person about whom it was recorded ask to see it**.

Data handling

All staff have a responsibility to handle the personal data which they come into contact with fairly, lawfully, responsibly and securely and in accordance with 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:

- Information and Records Retention and Security Policy;
- IT Acceptable Use Policy;
- Granville Staff Privacy Policy; and
- Granville GDPR Privacy Policy (Parents and Pupils).

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 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 PDPL. 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 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 they 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 PDPL, and to identity 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 Granville 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 DPO 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 PDPL as soon as possible.

Informing the individual

1 **Privacy Notice**: Individuals must be told what data is collected, and what it is used for, unless it is obvious. Staff and all parents have been provided with Privacy Notices, which explain what information will be collected, what it will be used for, which third parties (if any) it will be shared with and anything else which might be relevant. There is one for staff and another for parents and pupils. Copies of the school's privacy notices can be obtained from the school office and are stored on the school network in the staff area.

2 **Use:** Staff should inform the PDPL if they suspect that the School is using Personal Data in a way which might not be covered by an existing privacy notice.

Protecting confidentiality

1 **Disclosing Personal Data within the School:** Personal Data should only be shared on a need to know basis. Personal Data shall not be disclosed to anyone who does not have the appropriate authority to receive such information, irrespective of their seniority within the School or their relationship to the Data Subject, unless they need to know it for a legitimate purpose. Examples include:

1.1 the School Medical Assistant may disclose details of a lunchtime supervisor's allergy to bee stings to colleagues so that they will know how to respond, but more private health matters must be kept confidential;

1.2 personal contact details for a member of staff (e.g. their home address and telephone number, and their private mobile telephone number and email address) shall not be disclosed to parents, pupils or other members of staff unless the member of staff has given their permission.

2 **Disclosing Personal Data outside of the School:** Sharing Personal Data with others is often permissible so long as doing so is fair and lawful under the Regulations. However, staff should always speak to the PDPL if in doubt, or if staff are being asked to share Personal Data in a new way.

3 **Before sharing Personal Data outside of the School, staff should**:

3.1 make sure that they are allowed to share it;

3.2 ensure adequate security. What is adequate will depend on the nature of the data. For example, if the School is sending a child protection report to social services on a memory stick then the memory stick must be encrypted; and

3.3 make sure that the sharing is covered in the privacy notice.

4 **Digital Media:** The School should be careful when using photographs, videos or other media as this is subject to the Regulations as well, explicit parental consent is required for each pupil.

5 **Information security and protecting Personal Data:** Information security is the most important aspect of data protection compliance and most of the fines under the Regulations for non-compliance relate to security breaches.

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 from School premises, whether in paper or electronic form and wherever stored, without the 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/trustees or staff for official School business is not permitted.
- The School shall receive explicit written consent to share photos, videos or other images of staff or pupils online or on social media platforms.

Further information

30 **ICO website:** The School has registered its use of Personal Data with the Information Commissioner's Office and further details of the Personal Data it holds, and how it is used, can be found in the School's register entry on the Information Commissioner's website at www.ico.org.uk. This website also contains further information about data protection.

31 **Contact:** If you would like any further information about anything within this policy, please contact the Bursar or Compliance Officer.

Breach of this policy

32 A member of staff who deliberately or recklessly discloses Personal Data held by the School without proper authority could be found guilty of a criminal offence and gross misconduct. The latter of which could result in summary dismissal.

Linked Policies:

This policy should be read alongside the following:

- Information and Records Retention and Security Policy;
- IT Acceptable Use Policy;
- Granville Staff Privacy Policy; and
- Granville GDPR Privacy Policy (Parents and Pupils).