



Wetherby School Kensington Data Protection Policy

1. Background

Data protection is an important legal compliance issue for Wetherby School Kensington (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 Notices). The School, as data “controller”, is responsible for the actions of its staff and management team in how they handle data. It is therefore an area where all staff and representatives have a part to play in ensuring we comply with and are mindful of our legal obligations.

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. On this basis, a good principle 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 as to 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.

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 is a controller. An independent contractor who makes their own such decisions is also, separately, likely to be a controller.
- **Data Processor** – an organisation that processes personal data on behalf of a 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 data, including obtaining or collecting it, structuring it, analysing it, storing it, viewing it (including from a remote server), sharing it internally or with third parties (including making it available to be viewed electronically or otherwise), altering it or deleting it.
- **Profiling** - any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work or in School (for example, exam results), economic situation, health, personal preferences, interests, reliability, behaviour, location or movements
- **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 (broadly the same as for special category data).
- **Data protection authority** – the national authority responsible for the supervision of the implementation and protection of data and privacy as well as implementing and enforcing data protection law.

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, contractors or members of the management team of the School are obliged to comply with this policy when doing so. For employees, breaches of this policy may result in disciplinary action (including termination of employment). 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 controllers – which may range from other schools (including other schools within the Inspired Education Group (**Group**)), to parents and 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.

If you are a volunteer or contractor, you may 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.

4. Role of the Privacy Champion

The School has appointed Antonia Morant as its Privacy Champion. Questions about data protection training or the School's policies should be directed to the Privacy Champion in the first instance.

Please see below for who to contact in the event of an actual or suspected data breach or if you receive any kind of data protection related request or complaint from an individual.

5. The Principles

The School processes personal data in accordance with 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 '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 ("DPIAs") – see section below relating to DPIA); and
- generally having an 'audit trail' in respect of 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.

6. Lawful grounds for data processing

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 data protection law (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 (or third party). 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. When relying upon the School's legitimate interests, it is good practice to complete a Legitimate Interest Assessment (LIA) which can be used to determine if processing personal data on the basis of legitimate interests is justified – a template LIA can be requested from the Global DPO at dpo@inspirededu.com.

The School's legitimate interests are set out in its Privacy Notices, and include the School's interests in running the School in an efficient, professional, sustainable manner, in accordance with all relevant ethical, educational, legal and regulatory duties and requirements.

Other lawful grounds include:

- compliance with a legal obligation, including in connection with employment, engagement of services and diversity monitoring, for example an employer needs to process personal data to comply with its legal obligation to disclose employee salary details to the tax authority;
- contractual necessity, e.g. to perform a contract with staff or parents, or the engagement of contractors (e.g. debt collection of fees); and
- 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 such as safeguarding.

7. 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.

Finally, the School is required to keep and maintain and record of key processing activities under its responsibility – this should be recorded in the School's Record of Processing Activities (**ROPA**). Given that many of the larger processing activities are processed at a Group level, the Group also maintains a central Group ROPA which records such processing. The School will use its ROPA to record specific processing activity carried out at School level that is not captured in the Group ROPA.

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:

- The School's and the Group's (as applicable) IT policies, including the IT Acceptable Use Policy;
- Use of Images Policy;
- CCTV Policy;

- Data Retention Policy;
- Data Breach Policy;
- Data Protection Rights Policy;
- Safeguarding Policy; and
- Social Media Policy
- Mobile phones Policy
- Admissions 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.

As a general rule, all personal data received by a member of staff relating to other employees, pupils, parents, contractors, and other parties is private and should only be shared with staff members who have a legitimate need to know that information (i.e. on a “*need to know*” basis).

Avoiding, mitigating and reporting data breaches

One of the School’s key obligations is in relation to reporting personal data breaches. Controllers must report certain types of personal data breach (those which are likely to risk an impact to the rights and freedoms of individuals) to the data protection authority within 72 hours. In terms of assessing the severity of the breach, Controllers should consider a number of factors, including: (i) the type of personal data breach; (ii) the nature, sensitivity and volume of personal data affected; (iii) the severity of the consequences for the individuals affected; and (iv) the number of individuals affected.

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 data protection authority (which is a decision only to be made by the Global DPO and School DPO (if applicable)). All data breaches must be reported to the Global DPO who also maintains a central register of data incidents and breaches. If staff become aware of a personal data breach or suspect one may have occurred, they must notify the Group’s Global DPO at dpo@inspirededu.com and, if the School has one, the School’s external DPO. 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 Group 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 to the Global DPO (and the School’s external DPO, if applicable) could result in significant exposure for the School and could be a serious disciplinary matter, whether under this policy or the applicable staff member’s contract resulting to termination of employment.

Care and data security

The School uses appropriate security measures to ensure the security, confidentiality, integrity and privacy of the personal data it processes, which includes measures to prevent the unauthorised access or unlawful processing and the accidental loss, destruction or damage of personal data. This includes limiting access to certain information and restricting access to computer equipment through procedures that can identify and authenticate the user accessing them.

However, more generally, we require all School staff (and expect all our contractors) to remain mindful of the data protection principles (see section 3 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, including filing and sending correspondence, notably hard copy documents. For example, when documents are printed which contain personal data, those documents should be collected at once, or printed in a secure manner, making sure not to leave printed documents in the output tray. 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 lead by example and be culture carriers of these principles and to oversee the swift reporting of any concerns about how personal information is used by the School to the Group's Global DPO at dpo@inspirededu.com and (if applicable) School's external DPO, and to identify 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, including appropriate data processing provisions. 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) – please see the Group's separate policies on the use of AI. Any request to engage a third party supplier that involves material processing of personal data should be referred to the Global Head of Procurement and Global DPO in the first instance, and at as early a stage as possible.

Data Protection Impact Assessments (DPIA)

The School will be required in certain circumstances to carry out a DPIA. DPIAs are an essential tool which can help demonstrate the School's compliance with its accountability obligations. For example, DPIAs should be completed: (i) when onboarding a new supplier who will process personal data (e.g. a new piece of software that will process students' data); or (ii) if the School is doing something new with personal data.

When considering whether to complete a DPIA, you should ask:

- Am I using personal data in a new School system?
- Am I proposing to collect or use new types of personal data, including any sensitive personal data?
- Am I intending to collect or use personal data from new types of data subjects?
- Am I doing something with data in a way that a data subject (e.g. parents, pupils or staff) might not expect?

If the answer to any of the above questions is “Yes”, it is likely that a DPIA is required. In such circumstances, please contact the Global DPO and provide a detailed description of the proposed initiative. The Global DPO will then provide guidance and the correct DPIA template to complete.

8. 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 typically known as the 'subject access right' (or the right to make 'subject access requests'). Such a request must be dealt with promptly (normally within one month from the date of the request) and does not need any formality (i.e. the request can be made orally and does not

need to expressly state that it is a 'subject access request'), nor to refer to the correct legislation.

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 that legal basis 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, or making any kind of data protection related complaint you must tell the Group's Global DPO at dpo@inspirededu.com and, if the School has one, the School's external DPO, as soon as possible because data protection regulation sets strict time limits controllers for dealing with such request (typically within one month).

9. International Personal Data Transfers

Privacy regulations (such as the UK / EU GDPR) contains rules (and restrictions) on the transfer of personal to separate controllers or processors that are located in other countries. This is to ensure that the level of protection afforded to individuals is not undermined as a result of that transfer. Personal data originating in one country is transferred across borders when you transmit, send, view or access that data in or to a different country.

Transfers between the School and the Group are covered by a Data Sharing Agreement. However, if you are intending to transfer personal data to a third party which is located outside of the country you are located in, please notify the Global DPO before doing so, as this transfer may require a risk assessment and other contractual protections to ensure that the transfer is lawful.

10. 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. On this basis, all staff are required to comply with the terms of the Group's IT policies, including (but not limited to) the IT Acceptable Use Policy, Information Security Policy, and Mobile Devices and Social Media Policy, and in particular, the following data security rules:

- 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 Group's Global DPO and General Counsel.
- 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.
- Use of personal email accounts, personal devices or USBs by staff for official School business is not permitted. This includes sending personal data received or otherwise processed by the School to a personal email account.

Last Updated: May 2025