WESTMINSTER SCHOOL

DATA PROTECTION POLICY

Author: Elizabeth Wells
Lead: Bursar
Reviewer: Audit and Risk Committee

Date: May 2021
Review Date: May 2024

WESTMINSTER SCHOOL

DATA PROTECTION POLICY

INTRODUCTION

Data protection is an important legal compliance issue for Westminster School and not only seeks to ensure the welfare and safety of its pupils and staff, but also the security and efficient running of 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 governors, 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 they comply with and are mindful of their legal obligations, whether that personal data handling is sensitive or routine.

The law changed on Friday, 25 May 2018 with the implementation of the General Data Protection Regulation (GDPR) – an EU Regulation that continues to be directly effective in the UK – and the enactment of the Data Protection Act 2018 (DPA 2018) to deal with certain issues left for national law. 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.

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.

The School's registration under the DPA 2018 is: Z2553168. The school's registration details are available online from the ICO website and at the School by appointment.

DEFINITIONS

Key data protection terms used in this policy are as follows:

Data controller

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 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.

APPLICATION OF THIS POLICY

This policy sets out the School's expectations and procedures with respect to processing any personal data that might be collected from data subjects (including parents, pupils, employees, governors, 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 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.

Volunteers or contractors are data controllers in their own right, but the same legal regime and best practice standards set out in this policy will apply to them by law.

PERSONS RESPONSIBLE FOR DATA PROTECTION

The School has appointed as the Data Controllers the Head Master (or the Master of the Under School as appropriate) for matters relating to pupils and the Bursar for matters relating to the administration. The Governing Body, Head Master, Master and Bursar will endeavour to ensure that all personal data is processed in compliance with this policy and the principles of the DPA 2018. They are responsible for:

- Responding to any subject access requests.
- Checking and approving third parties that handle the School's data.

The Archivist and Records Manager acts as a Data Protection Adviser and they are responsible for:

- Keeping the Governing Body, SMC of Westminster Great School and SMT of Westminster Under School updated about data protection responsibilities, risks and issues.
- Reviewing data protection procedures and policies on a regular basis.
- Arranging data protection training.
- Providing advice and guidance to staff and the Governing Body.

The Director of Digital Strategy and IT is responsible for:

- Ensuring all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Researching third-party services, such as cloud services that the School uses to store or process data.

Together the Bursar, Director of Digital Strategy and IT, and Archivist and Records Manager form the Data Protection Team and can be contacted should there be any queries or concerns regarding personal data.

All staff (and including governors and contractors) involved with the collection, processing and disclosure of personal data must adhere to the following principles:

- Staff should only ever share information on a "need to know basis"; seniority does not give an automatic right to information.
- Data protection should never be used as an excuse for not sharing information where necessary. The welfare of the child is paramount.
- Records of any sort (and particularly email), could at some point in the future be disclosed, whether as a result of litigation or investigation, or because of a subject access request under the DPA 2018. Therefore, when recording information, accuracy, clarity and objectivity should be paramount.
- Personal data should be retained only as long as is necessary and destroyed securely.
- No member of staff is permitted to remove sensitive personal data from School premises, whether in paper or electronic form with two exceptions:
    - The School's pupil database and staff email may be accessed on personal devices provided that the device is secure and password protected.
    - For pupils on residential trips, medical information and other relevant information (e.g.: passport details) may be taken off site by the trip leader.

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 School not only processes personal data in a fair and legal manner but that the School is also able to demonstrate that its processing is lawful. This involves, among other things:

- Keeping records of data processing activities, including by way of logs and policies.
- Documenting significant decisions and assessments about how the School uses personal data (including via formal risk assessment documents called Data Protection Impact Assessments).
- Having an "audit trail" vis-à-vis data protection and privacy matters, including, for example:
    - When and how the School's Privacy Notices are 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 as 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 FOR 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 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 that 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 with which they come into contact 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. 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 there is a need to notify the ICO. If staff become aware of a personal data breach then they must notify the Data Protection Team by completing a data breach report via the Intranet homepage (under "Data Breach Reporting"). 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, all School staff are required and all contractors expected to remain mindful of the data protection principles (see 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 affects daily processes, such as filing and sending correspondence, notably hard copy documents. Data handlers should always consider what the most assured and secure means of delivery might be, and what the consequences would be of loss or unauthorised access.

The School expects 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 Data Protection Team, and to identity the need for (and implement) regular staff training. Staff must attend any training required.

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 a member of staff becomes aware of a subject access request (or indeed any communication from an individual about their personal data), the Head Master, Master or Bursar must be informed as soon as possible.

Requests from pupils will be processed as any subject access request and information will be given directly to the pupil, unless it is clear that the pupil does not understand the nature of the request. In general, the School will assume that pupils' consent to disclosure of their personal data to their parents (e.g.: for the purposes of keeping parents informed about the pupil's activities, progress and behaviour, and in the interests of the pupil's welfare), unless, in the School's opinion, there is a good reason to do otherwise.

However, where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents, the School will maintain confidentiality unless, in the School's opinion, there is a good reason to do otherwise (e.g.: where the School believes disclosure will be in the best interests of the pupil or other pupils).

Individuals also have legal rights to:

- Require the School to correct the personal data held about them if it is inaccurate;
- Request the erasure of their personal data (in certain circumstances);
- Request the restriction of the School's data processing activities (in certain circumstances);
- Receive from the School the personal data held 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 the School's 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 the School is relying on it for processing 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 a member of staff receives a request from an individual who is purporting to exercise one or more of their data protection rights, you must tell the Head Master, Master or Bursar must be informed as soon as possible.

ENFORCEMENT
This Policy forms part of the terms and conditions of all employees' contracts of employment. A breach of the policy may be regarded as misconduct, leading to disciplinary action up to and including summary dismissal. It also applies to all members of the Governing Body and other officers of the School and breach of this Policy may result in appropriate action being taken by the School.

QUERIES AND COMPLAINTS
Any comments or queries on this Policy should be directed to the Data Controllers in writing using the following contact details:

The Bursar
Westminster School
17 Dean's Yard,
London
SW1P 3PB

If an individual believes that the School has not complied with this Policy or acted otherwise than in accordance with the DPA 2018, they should also notify the Data Controllers.

Further information about the DPA 2018 can be obtained from the Data Protection Commissioner (Information Line 01625 545 745, website www.dataprotection.gov.uk).

ANNEX A

DATA SECURITY PRINCIPLES

- Access to personal data is provided to members of staff who require access to that personal data to perform their duties and responsibilities. As a result, different members of staff will have access to different categories of personal data depending upon their role.

- The security measures in place to protect data held electronically are set out in the Acceptable Use of Computer Network by Staff and Acceptable Use of Computer Network by Pupils Policies, which are reviewed regularly. All data on the Westminster networks is protected by anti-virus software that runs on servers and workstations, and is updated automatically. Data on the network is backed-up daily.

- Personal data held in manual files is only accessible by authorised individuals and, where of a confidential nature, is kept in locked filing cabinets when not in use.

- Paper-based copies of personal data (or other sensitive or confidential data) are disposed of in a secure manner, by shredding. Decommissioned IT equipment has data destruction procedures applied prior to its disposal.

- The physical security of the School premises is checked by the Security Department daily.

- The School ensures that, prior to the transfer of any personal data to a third party for processing, the third party has appropriate technical and organisational security measures governing the processing to be carried out.

- New staff are required to read and understand the Acceptable Use Policy as part of their induction.

- Any lapses in data security must be reported to the Director of Digital Strategy and IT at the earliest opportunity.