WESTMINSTER SCHOOL

DATA PROTECTION POLICY

Author: Elizabeth Wells
Lead: Bursar

Date: May 2018
Review Date: May 2021

WESTMINSTER SCHOOL

DATA PROTECTION POLICY

INTRODUCTION

Westminster School needs to collect and use certain types of personal information in order to operate. Subjects include current, past and prospective employees, pupils, supporters, suppliers, clients, and others with whom the school communicates. In addition, it may be required by law to collect and use certain types of information to comply with the requirements of government departments. This personal information must be handled correctly - whether on paper, in a computer, or recorded on other material - and there are safeguards to ensure this in the Data Protection Act 2018.

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

RESPONSIBILITIES

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 and Bursar** will endeavour to ensure that all personal data is processed in compliance with this Policy and the Principles of the DPA. They are responsible for responding to any subject access requests and checking and approving third parties that handle the School's data.

The **Archivist and Records Manager** acts as a **Data Protection Adviser**, keeping the Governing Body and Senior Management Committee updated about data protection responsibilities, risks and issues. They are also responsible for reviewing data protection procedures and policies on a regular basis; arranging data protection training; and 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; and researching third-party services, such as cloud services the School is considering using to store or process data.

All staff 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. 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.

DATA AUDIT AND REGISTER

The School completes regular data audits and maintains a register of what data is held, where it is stored, how it is used, the conditions for processing, who is responsible and any further regulations or retention timescales that may be relevant. This register is accessible on application.

PRINCIPLES

The School adheres to the principles of DPA. Personal data will be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

PRESONAL DATA PROCESSED BY THE SCHOOL

Personal data processed by the School includes the following:

- names, addresses, telephone numbers, e-mail addresses and other contact details;
- bank details, employment details, family circumstances and other financial information, eg. about parents who pay fees to the School;
- past, present and prospective pupils' academic, disciplinary, admissions and attendance records (including information about any special educational needs), and examination scripts and marks;
- where appropriate, information about individuals' health, and contact details for their next of kin;
- references given or received by the School about pupils, and information provided by previous educational establishments and/or other professionals or organisations working with pupils; and

- images, audio and video recordings of pupils (and occasionally other individuals) engaging in school activities, and images captured by the school's CCTV system.

Generally, the School receives personal data from the individual directly (or, in the case of pupils, from parents). However, in some cases personal data may be supplied by third parties (for example another school, or other professionals or authorities working with that individual and the Disclosure and Barring Service), or collected from publicly available resources.

PURPOSES FOR WHICH DATA MAY BE PROCESSED

The School will use (and where appropriate share with third parties) personal data about individuals for a number of purposes as part of its operations, including as follows:

- For pupil selection including the registration of prospective pupils and administration of the admissions process;
- For provision of educational support and ancillary services including school curriculum and timetable, pastoral care, SEN support, health care services and maintenance of discipline; careers and library services; administration of sports fixtures and teams, school trips; and boarding house administration;
- For the purposes of management planning and forecasting, research and statistical analysis, and to enable the relevant authorities to monitor the school's performance;
- To give and receive information and references about past, current and prospective pupils, including relating to outstanding fees or payment history, to/from any educational institution that the pupil attended or where it is proposed they attend; and to provide references to potential employers of past pupils;
- To enable pupils to take part in national or other assessments, and to publish the results of public examinations or other achievements of pupils of the school;
- To safeguard pupils' welfare and provide appropriate pastoral (and where necessary, medical) care, and to take appropriate action in the event of an emergency or accident, including by disclosing details of an individual's medical condition where it is in the individual's interests to do so, for example for medical advice, insurance purposes or to organisers of school trips.
- To monitor (as appropriate) use of the school's IT and communications systems in accordance with the school's IT acceptable use policies;
- To make use of photographic images of pupils in school publications, on the school website and (where appropriate) on the school's social media channels;
- For the protection and promotion of the School’s legitimate interests and objectives including the publication of its own websites, its internal communication system and virtual learning environment, the prospectus, Almanack and other publications; fund-raising for the School’s charitable purposes; the maintenance of a historic archive; and communicating with the body of current and former pupils and/or their parents or guardians.
- For security purposes, and for regulatory and legal purposes (for example child protection and health and safety) and to comply with its legal obligations;
- The administration of its staff, agents and suppliers including the recruitment of staff/ engagement of contractors (including compliance with DBS procedures); administration of payroll, pensions and sick leave and the maintenance of appropriate human resources records for current and former staff; and providing references; and
- Where otherwise reasonably necessary for the school's purposes, including to obtain appropriate professional advice and insurance for the school.

THIRD PARTIES WITH WHOM THE SCHOOL MAY NEED TO PASS PERSONAL DATA

From time to time the School may pass personal data (including sensitive personal data where appropriate) to third parties, including local authorities, other public bodies (eg the DBS, UK Border Agency, HM Revenue and Customs, Department for Education and Department for Work and Pensions), independent school bodies such as the Independent Schools Inspectorate and the Independent Schools Council, school doctors and other health professionals, the School’s

professional advisers. The school maintains an up-to-date register of third parties which it uses to process data on its behalf.

RIGHTS OF DATA SUBJECTS

Access

The DPA extends to all data subjects a right of access to their own personal data. In order to ensure that people receive only information about themselves it is essential that a formal system of requests is followed. Subject Access Requests should be in writing and referred to the Head Master, Master or the Bursar as appropriate. It may be necessary for the individual submitting the request to provide verification of their identity. The School will endeavour to respond to any such written requests as soon as is reasonably practicable and in any event, within 1 month for access to records under the DPA. Upon request, a data subject should have the right to receive a copy of their data in a structured format.

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 the case of any written request from a parent regarding their own child's record, access to the record will be provided within 15 school days in accordance with the current Education (Pupil Information) Regulations. A pupil of any age may ask a parent or other representative to make a Subject Access Request on his behalf.

In general, the School will assume that pupils consent to disclosure of their personal data to their parents, eg. 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; for example, where the School believes disclosure will be in the best interests of the pupil or other pupils.

Exemptions

You should be aware that certain data is exempt from the right of access under the DPA. This may include information which identifies other individuals, information which the School reasonably believes is likely to cause damage or distress, or information which is subject to legal professional privilege.

The school is also not required to disclose any pupil examination scripts (though examiners' comments may, in certain circumstances, be disclosed), nor any reference given by the school for the purposes of the education, training or employment of any individual.

Accuracy

The school will endeavour to ensure that all personal data held in relation to an individual is as up to date and accurate as possible. Individuals must notify the School of any changes to information held about them. An individual has the right to request that inaccurate information about them is erased or corrected (subject to certain exemptions and limitations under the Act) and may do so by contacting the Head Master, Master or Bursar in writing.

Right to be Forgotten

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

Personal Data Breach

A personal data breach is “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service”. A personal data breach may mean that someone other than the school gets unauthorised

access to personal data. But a personal data breach can also occur if there is unauthorised access within the school or if a member of staff accidentally alters or deletes personal data.
All members of staff have an obligation to report actual or potential data protection compliance failures no more than 24 hours of becoming aware of the breach. This notification must include at least:

- your name and contact details;
- the date and time of the breach (or an estimate);
- the date and time you detected it;
- basic information about the type of breach; and
- basic information about the personal data concerned.

This allows the school to investigate the failure and take remedial steps if necessary; maintain a register of compliance failures; and notify the Information Commissioners Office and any affected parties of the breach.

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 Act, they should also notify the Data Controllers.
Further information about the Data Protection Act 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 School Acceptable Use Policy, which is reviewed annually. 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.