AVON HOUSE
PREPARATORY SCHOOL

CELEBRATING & SUPPORTING EVERY CHILD

Data Protection Policy

Introduction

The School respects everyone's right to privacy. An established procedure for dealing with confidentiality, which is understood by pupils, staff, parents, carers and visitors, will help the School develop a more consistent approach and protect the interests of both its pupils and staff.

Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, advisors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018) This policy applies to all personal data, regardless of whether it is in paper or electronic format.

Area of School

This policy covers the whole school community.

The Data Controller

Avon House School processes personal data relating to parents, pupils, staff, advisers, visitors and others, and therefore is a data controller. The School is registered as a data controller with the Information Commissioner's Office (ICO) and will renew this registration annually or as otherwise legally required. The School's registration number is Avon House School – Z6834898.

Data Protection Officer

The School has appointed a DPO to ensure GDPR Compliance. The DPO is responsible for overseeing this Data Protection Policy and developing data-related policies and guidelines. In Avon House School the DPO is the Bursar, Mr N Best and he is contactable by email: bursar@ahsprep.co.uk or by post: Bursar, Avon House Preparatory School, 490 High Road, Woodford Green, Essex IG8 0PN

Responsibilities and Accountability

The proprietary body has overall responsibility for ensuring that the School complies with all relevant data protection obligations.

The Governors have an oversight role for ensuring compliance with the School's Data Protection policy.

This policy applies to all staff employed by our school, and to external organisations or individuals working on our behalf. Members of staff who do not comply with this policy may face disciplinary action.

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the School of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
  - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
  - If they have any concerns that this policy is not being followed
  - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
  - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
  - If there has been a data breach
  - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
  - If they need help with any contracts or sharing personal data with third parties

Training

All staff receive Data Protection training and this will also form part of their continuing professional development.

Principles

The School is responsible for and adheres to the principles relating to the processing of personal data as set out in the GDPR.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the School aims to comply with these principles.

CELEBRATING & SUPPORTING EVERY CHILD

Lawful Bases

The School will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can fulfil a contract with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, can perform a task in the public interest, and carry out its official functions
- The data needs to be processed for the legitimate interests of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent

Special Category Data (Sensitive Personal Information)

The School may only process special category data if they are entitled to process personal data (using one of the fair processing conditions above) AND one of the following conditions are met:

- The data subject has given their explicit consent;
- The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed on the School in the field of employment law, social security law or social protection law. This may include, but is not limited to, dealing with sickness absence, dealing with disability and making adjustments for the same, arranging private health care insurance and providing contractual sick pay;
- To protect the data subject's vital interests;
- To meet our legal compliance obligations (other than a contractual obligation);
- Where the data has been made public by the data subject;
- To perform a task in the substantial public interest or in order to carry out official functions as authorised by law;
- Where it is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services;
- Where it is necessary for reasons of public interest in the area of public health;
- The processing is necessary for archiving, statistical or research purposes.

The School identifies and documents the legal grounds being relied upon for each processing activity.

CELEBRATING & SUPPORTING EVERY CHILD

Consent

Where the School relies on consent as a fair condition for processing (as set out above), it will adhere to the requirements set out in the GDPR.
Consent must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they signify agreement to the processing of personal data relating to them. Explicit consent requires a very clear and specific statement to be relied upon (i.e. more than just mere action is required).

A data subject will have consented to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity will not amount to valid consent.

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured.

If explicit consent is required, the School will normally seek another legal basis to process that data. However if explicit consent is required, the data subject will be provided with full information in order to provide explicit consent.

The School will keep records of consents obtained in order to demonstrate compliance with consent requirements under the GDPR.

Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary. Staff must only process personal data where it is necessary in order to do their jobs. When staff no longer require the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with legal timeframes for retaining data.

Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils, for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law.

- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share.
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

There may be circumstances where the School is required either by law or in the best interests of our pupils, parents or staff to pass information onto external authorities, for example, the local authority, Department of Education, ISA or Government Departments. These authorities have their own policies relating to the protection of any data that they receive or collect.

The intention to share data relating to individuals to an organisation outside of our School shall be clearly defined within written notifications and details and basis for sharing that data given.

Rights and Requests

Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the School holds about them. This could include:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.
- Subject access requests must be submitted in writing, either by letter or email to the DPO. They should include:
- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested. Should staff receive a subject access request they must immediately forward it to the DPO.

Data Protection Rights

Personal data must be made available to data subjects as set out within this policy and data subjects must be allowed to exercise certain rights in relation to their personal data. The rights data subjects have in relation to how the School handles their personal data are set out below: -

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO (although the ICO recommends that steps are taken to resolve the matter with the School before involving the regulator)
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

Data Protection Impact Assessments (DPIA's)

Where processing is likely to result in a high risk to an individual's data protection rights (eg where the School is planning to use a new form of technology) we will, before commencing the processing, carry out a DPIA to assess:

- Whether the processing of data is necessary and proportionate in relation to its purpose
- The risks to individuals
- What measures can be put in place to address those risks and protect personal information
- Before any new form of technology is introduced, the person responsible should therefore contact the DPO in order that a DPIA can be carried out
- During the course of any DPIA, the employer will seek the advice of the DPO and any other relevant stakeholders

Privacy notice

The School will issue privacy notices from time to time, informing members of the school community about the personal information that they collect and hold relating to them, how they can expect their personal information to be used and for what purposes.

We will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

CELEBRATING & SUPPORTING EVERY CHILD

Personal Data Breaches

The GDPR requires the School to notify any applicable personal data breach to the ICO. We have put in place procedures to deal with any suspected personal data breach and will notify data subjects or any applicable regulator where we are legally required to do so. If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself and immediately contact the Head Teacher or DPO.

Disposal of Data

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Data Security and storage

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage, using the following measures:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice or display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site it must be safeguarded, papers should be carried in locked briefcases. Staff should only use the encrypted USB sticks provided by the school.
- Passwords that are at least 8 characters long are used to access school computers, laptops and other electronic devices.

Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

CCTV

Should the School introduce CCTV in various locations around the school site we will ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV. We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use. Any enquiries about the CCTV system should be directed to the Head Teacher.

CELEBRATING & SUPPORTING EVERY CHILD

Monitoring

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed every year or if any changes are made to the Data Protection Act 2018.

Policy links

This policy should be read in conjunction with the School's:

- Privacy Notice
- Taking, Storing and Using Images of Children Policy
- Safeguarding Policy
- Acceptable Use Policy
- E-Safety Policy
- Staff Use of Social Media and Networking Sites Policy

September 2018 NB
Reviewed August 2019 NB