AVANTI SCHOOLS TRUST

Data Protection

May 2018

Next Review Date: May 2019

Data Protection*

Contents

Policy statement and Objectives

The objectives of this Data Protection Policy are to ensure that Avanti Schools Trust (the "Trust") and its directors, governors and employees are informed about, and comply with, their obligations under the Data Protection Act 1998 ("the Act"). The policy has also been updated to incorporate changes flowing from the General Data Protection Regulations which come into force on the 25th of May 2018.

Everyone has rights with regard to how their personal information is handled. During the course of our activities we will collect, store and process personal information about a number of different groups of people and we recognise the need to treat it in an appropriate and lawful manner.

The types of information that we may be required to handle include details of current, past and prospective employees and pupils, parents, directors, governors, suppliers and other individuals that we communicate with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Act and other regulations. The Act imposes restrictions on how we may use that information. This policy does not form part of any employee's contract of employment and it may be amended at any time. Any breach of this policy will be taken seriously and may result in disciplinary action and serious breaches may result in dismissal. Breach of the Act may expose the Trust to enforcement action by the Information Commissioner or fines. Furthermore, certain breaches of the Act can give rise to personal criminal liability for the Trust's employees. At the very least, a breach of the Act could damage our reputation and have serious consequences for the Trust.

The Trust has notified the Information Commissioner that it processes personal information, and is on the register of data controllers, registration number 07506598. For the purposes of the Act, the School is the Data Controller.

Status of the policy

This policy has been approved by the Directors of the Trust. It sets out our rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information. The Data Controllers are responsible for ensuring compliance with the Act and with this policy. Any questions or concerns about the operation of this policy should be referred in the first instance to dataprotection@avanti.org.uk.

Definition of terms

Data is information which is stored electronically, on a computer, or in certain paper-based filing systems.

Data subjects for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a school report) and can include telephone numbers, photographs and CCTV images.

Data controllers are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. We are the data controller of all personal data used in our business.

Data users include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.

Data processors include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition, but it could include suppliers which handle personal data on our behalf.

Parent has the meaning given in the Education Act 1996 and includes any person having parental responsibility or care of a child.

Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions and will usually require the express consent of the person concerned.

Data protection principles

Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

- Processed fairly and lawfully.
- Processed for limited purposes and in an appropriate way.
- Adequate, relevant and not excessive for the purpose.
- Accurate.

- Not kept longer than necessary for the purpose.
- Processed in line with data subjects' rights.
- Secure.
- Not transferred to people or organisations situated in countries without adequate protection.

Fair and lawful processing

The Act is intended not to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is (in this case the School), the purpose for which the data is to be processed by us, and the identities of anyone to whom the data may be disclosed or transferred.

For personal data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, more than one condition must be met. In most cases the data subject's explicit consent to the processing of such data will be required.

Processing for limited purposes

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected, or for any other purposes specifically permitted by the Act. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs.

Adequate, relevant and non-excessive processing

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

In order to ensure compliance with this principle, the Trust will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data. Decisions on data to be deleted must come from the Data Controller, after taking appropriate guidance.

Accurate data

Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

If a data subject informs the Trust of a change of circumstances their computer record will be updated as soon as is practicable. A printout of their data record will be provided to data subjects periodically so they can check its accuracy and make any amendments.

Where a data subject challenges the accuracy of their data, the Trust will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Board of Directors for their judgement. If the problem cannot be resolved at this stage, the data subject should refer their complaint to the Information Commissioner's Office. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.

Notwithstanding the above paragraph, a data subject continues to have rights under the Act and may refer a complaint to the Information Commissioner's Office.

Sensitive personal data

The School acknowledges it has special obligations in connection with the use of Sensitive Personal Data, namely information about an individual's race, ethnic origin, political or religious beliefs, trade union membership, health, sex life and actual or alleged criminal activity.

Biometric Data

Biometric information is used in some cases by the school to facilitate daily cashless catering transactions. In due course it may also be extended to other services (e.g. library) and where this is the case the School shall notify parents. Biometric data that is collected by the school is processed in accordance with the Data Protection Act 1998.

Timely processing and Retention

Personal data should not be kept longer than is necessary for the purpose for which it is held. This means that data should be destroyed or erased from our systems when it is no longer required.

It is the duty of the Data Controller, after taking appropriate guidance for legal considerations, to ensure that obsolete data are properly erased. The Trust has a retention schedule for all data.

<u>Students</u>
The school will retain personal data securely and only in line with how long it is necessary to keep for a legitimate and lawful reason. Typically, the legal recommendation for how long to keep ordinary pupil personnel files is up to 7 years following departure from the school. However, incident reports and safeguarding files will need to be kept much longer, in accordance with specific legal requirements. If you have any specific queries about how this policy is applied, or wish to request that personal data that you no longer believe to be

relevant is considered for erasure, please contact the School. However, please bear in mind that the school may have lawful and necessary reasons to hold on to some data.

Staff Records

Staff Records Paper files on teaching personnel are held by the Principal, HR Dept and members of the Senior Management Team as required. They mainly comprise information on the teaching qualifications and experience of teaching staff but some personal details are included. After the member of staff has left the School the personnel file is retained at the school for 7 years unless there has been a safeguarding allegation then the data is held for 25 years.

The HR Dept maintains files on all staff, both teaching and support. They mainly comprise information on the recruitment and employment of the staff member including pay, training, sickness and disciplinary records. All pension and payroll information is held directly with the 3rd party provider.

Records relating to unsuccessful candidates are held for 6 months after the date of interviews and then destroyed. If it is the intention to retain data on any unsuccessful candidate for longer than this period they must be notified of this intention and given the opportunity to object.

Records relating to unsuccessful candidates are held for 6 months after the date of appointment and then deleted or destroyed. If it is the intention to retain data on any unsuccessful candidate for longer than this period they must be notified of this intention and given the opportunity to object.

Monitoring and Communications

The School respects the individual's right to privacy. It is the policy of the School that it will not actively intercept or monitor individual communications. Overall use of the School's communication systems is monitored to ensure that there is: no unauthorised use of the systems; use is relevant to the School's business; systems are operating effectively.

For practical purposes this means that:

- Telephone conversations will not be monitored but the time and duration of calls made, including the number of the recipient, may be logged.

- Use of the world wide web will be monitored to protect systems from viruses and to ensure that use is suitable for a school.

- As a general principle, staff use of the School email system is not private. Individual emails will not, in normal circumstances, be opened but users must recognise that, even when they have deleted an email, a copy may still reside in the system for some time. Information sent by normal email is not secure and the reasons for this are beyond the control of the School.

• If a member of staff is absent for a long period and it is thought to be relevant to the School's business to open emails then efforts will be made to obtain consent beforehand.

• Abuse of the School's communication systems is a disciplinary offence.

Processing in line with data subject's rights

Data must be processed in line with data subjects' rights. Data subjects have a right to:
Request access to any data held about them by a data controller;
Prevent the processing of their data for direct-marketing purposes;
Ask to have inaccurate data amended; and
Prevent processing that is likely to cause damage or distress to themselves or anyone else.

Data security

The Trust has taken steps to 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. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.

The Act requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if they agree to comply with those procedures and policies, or if they put in place adequate measures themselves.

Consideration should be given as to whether contracts with third party data-processors contain suitable contractual obligations on the third party to comply with the Act and to indemnify the Trust for if they breach the Act.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

Confidentiality means that only people who are authorised to use the data can access it.

Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.

Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our central computer system instead of individual PCs.

Security procedures include:

Physical Security
Appropriate building security measures are in place, such as alarms, window bars, deadlocks and computer hardware cable locks. Disks, tapes and printouts are locked away securely when not in use. Visitors to the School are required to sign in and out, to wear

identification badges whilst in the School and are, where appropriate, accompanied. Any stranger seen in entry-controlled areas should be reported.

Computer Security
Security software is installed on all computers containing personal data. Only authorised users are allowed access to the computer files and password changes are regularly undertaken. Computer files are backed up (i.e. security copies are taken) regularly. Data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

Procedural Security
In order to be given authorised access to the computer, staff will have to undergo checks and will be familiar with the IT acceptable use policy as set out in our Staff HR Handbook. All staff are trained in their Data Protection obligations and their knowledge updated as necessary. Computer printouts as well as source documents are shredded before disposal.

Paper documents should be shredded and floppy disks and CD-ROMs should be given to the IT department to be physically destroyed when they are no longer required.
The Trust has a Bring Your Own Device policy for employees to sign where personal data held by the Trust is processed on their personal mobile phones, tablets, computers or other devices.

Dealing with subject access requests

The Act extends to all data subjects a right of access to their own personal data. A formal request from a data subject for information that we hold about them must be made in writing. Any member of staff who receives a written request should forward it to their line manager or the Data Controller **IMMEDIATELY** as there are statutory time limits for responding (currently 30 calendar days).

In order to ensure that people receive only information about themselves it is essential that a formal system of requests is in place.

Where a request for subject access is received from a pupil, the Trust's policy is that:

a) Requests from pupils who are considered mature enough to understand their rights under the Act will be processed as a subject access request as outlined below and the data will be given directly to the pupil (subject to any exemptions that apply under the Act or other legislation). The Information Commissioner's guidance is that it may be reasonable to adopt a presumption that by the age of 12 a child has sufficient maturity to understand their rights and to make an access request themselves if they wish. In every case it will be for the Trust, as data controller, to assess whether the child is capable of understanding their rights under the Act and

the implications of their actions, and so decide whether the parent needs to make the request on the child's behalf. A parent would normally be expected to make a request on a child's behalf if the child is younger than 12 years of age.

b) Requests from pupils who do not appear to understand the nature of the request will be referred to their parents or carers.

c) Requests from parents in respect of their own child will be processed as requests made on behalf of the data subject (the child) and the data will be sent in a sealed envelope to the requesting parent (subject to any exemptions that apply under the Act or other legislation) unless the Trust considers the child to be mature enough to understand their rights under the Act, in which case the Trust shall ask the child for their consent to disclosure of the personal data (subject to any enactment or guidance which permits the Trust to disclose the personal data to a parent without the child's consent). Subject to paragraph 14, if consent is not given to disclosure, the Trust shall not disclose the personal data if to do so would breach any of the eight data protection principles.

It should be noted that the Education (Pupil Information) (England) Regulations 2005 do not apply to academies so the rights available to parents in those Regulations to access their child's educational records are not applicable to schools in the Trust. Instead, requests from parents for personal data about their child must be dealt with under the Act (as outlined above). This is without prejudice to the obligation on the Trust in the Education (Independent School Standards) (England) Regulations 2014 to provide an annual report of each registered pupil's progress and attainment in the main subject areas taught to every parent (unless they agree otherwise in writing).

Following receipt of a subject access request, and provided that there is sufficient information to process the request, an entry will be made in the Trust's Subject Access log book, showing the date of receipt, the data subject's name, the name and address of requester (if different), the type of data required (e.g. Student Record, Personnel Record), and the planned date for supplying the information (not more than 30 days from the request date). Should more information be required to establish either the identity of the data subject (or agent) or the type of data requested, the date of entry in the log will be date on which sufficient information has been provided.

Providing information over the telephone

Any member of staff dealing with telephone enquiries should be careful about disclosing any personal information held by us whilst also applying common sense to the particular circumstances. In particular, they should:
Check the caller's identity to make sure that information is only given to a person who is entitled to it.

Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.

Refer to their line manager or the Data Controller for assistance in difficult situations. No-one should be bullied into disclosing personal information.

Authorised disclosures

The School will, in general, only disclose data about individuals with their consent or unless the law requires or allows us to. There are circumstances under which the Trust may need to disclose data without explicit consent for that occasion including (but not limited to) the following:

a) Pupil data disclosed to authorised recipients related to education and administration necessary for the Trust to perform its statutory duties and obligations.

b) Pupil data disclosed to authorised recipients in respect of their child's health, safety and welfare.

c) Pupil data disclosed to parents in respect of their child's progress, achievements, attendance, attitude or general demeanour within or in the vicinity of the Trust.

d) Staff data disclosed to relevant authorities e.g. in respect of payroll and administrative matters.

e) Unavoidable disclosures, for example to an engineer during maintenance of the computer system. In such circumstances the engineer would be required to sign a form promising not to disclose the data outside the Trust.

f) Disclosures required as a result of a court order or pursuant to an act of Parliament.

g) Disclosures to the Police where the Trust is satisfied that the information is needed to prevent or detect a crime or to catch and prosecute a suspect.

14.2 Only authorised and trained staff are allowed to make external disclosures of personal data in accordance with the Act. Data used within the Trust by administrative staff, teachers and welfare officers will only be made available where the person requesting the information is a professional legitimately working within the School who needs to know the information in order to do their work.

CCTV

Where applicable the School will have CCTV procedures and guidelines in place. These can be found in the Schools Policies.

Policy Review

It is the responsibility of the Directors to facilitate the review of this policy on a regular basis. Recommendations for any amendments should be reported to the Data Protection Officer.

We will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives.

Enquiries

Further information about the School's Data Protection Policy can be found by emailing dataprotection@avanti.org.uk.

General information about the Act can be obtained from the Information Commissioner's Office: www.ico.gov.uk.

Useful References

The Information Commissioner's Office
https://ico.org.uk/