THE AVON VALLEY SCHOOL AND PERFORMING ARTS COLLEGE

DATA PROTECTION POLICY

Date of policy: January 2023
Date of next review: January 2025

RATIONALE

The Avon Valley School collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with it's statutory obligations.

Schools have a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website. Schools also have a duty to issue a Fair Processing Notice to all pupils/parents; this summarises the information held on pupils, why it is held and the other parties to whom it may be passed on.

Additional Information

The EU's GDPR has been amended into a new "**UK-GDPR**" (United Kingdom General Data Protection Regulation) that took effect on January 31, 2020. The **Data Protection Act 2018** has been amended to be read in conjunction with the new UK-GDPR instead of the EU GDPR. The European GDPR will apply to the UK in the **transition period** lasting from January 31, 2020 until December 31, 2020 (unless further extensions are agreed upon between the UK and EU). It is likely that the UK government will move to consolidate the two amended laws (UK-GDPR and Data Protection Act 2018) into one, comprehensive piece of data protection law at a later point

PURPOSE

Our school aims to ensure that all personal data collected about staff, students, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.:

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

WHAT IS PERSONAL INFORMATION?

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held.

This may include the individual's:

- Name (including initials)
- Identification number
- Location data
- Online identifier, such as a username

Some personal data is classed as being more sensitive and so needs more protection. Special Category Data may include:

- Data on children's services interactions
- Free School Meal (FSM) Status
- Pupil Premium (PP) eligibility
- SEN info
- Safeguarding information
- Student behaviour data
- Student attendance data

(Please note the list above is not exhaustive)

DATA PROTECTION PRINCIPLES

The GDPR is based on data protection principles that our school must comply with.

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.

COLLECTING PERSONAL DATA

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, as a public authority, 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**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If the School offers online services to pupils, such as classroom apps, and intends to rely on consent as a basis for processing, the School will get parental consent where the pupil is under 13 (except for online counselling and preventive services).

Whenever the School first collects personal data directly from individuals, we will provide them with the relevant information required by data protection law.

BIOMETRIC DATA

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, students use finger prints to receive school dinners instead of paying with cash, we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and students have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those students. For example, students can pay for school dinners in cash at each transaction if they wish.

Parents/carers and students can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a student refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the student's parent(s)/carer(s).

INFORMATION SECURITY

All portable electronic devices should be kept as securely as possible on and off school premises. If they contain personal information, they should be kept under lock and key when not in use. This is a legal requirement if they hold personal information that could be considered confidential.

Memory sticks and any type of portable storage should not to be used to store personal information. For more information regarding the use of memory sticks, refer to the school's ICT Acceptable Use Policy.

Whenever possible, storage rooms, strong cabinets and other storage systems with locks should be used to store paper records. Papers containing personal information should not be left on office and classroom desks, on staffroom tables or pinned to noticeboards where there is general access. Particular care should be taken if documents have to be taken out of school.

SHARING PERSONAL INFORMATION

Sharing personal information involves providing it to another organisation or person so that they can make use of it. It does not extend to the use of personal information within the school, including use by the governing body.

The main organisations that the school shares personal data with are:

- Local authorities
- Other schools and educational bodies
- Social services

The three most important aspects to consider when sharing data are:

- Making sure you are allowed to share it
- Ensuring that adequate security (taking into account the nature of the information) is in place to protect it
- Providing an outline in a fair processing notice of who receives personal information from the school.

If you send an email containing personal data from a secure server to an insecure recipient, security will be threatened. You may need to check that the recipient's arrangements are secure enough before sending your message.

For more information regarding the use of email to send personal data, refer to the school's ICT Acceptable Use Policy.

COMPLAINTS

Complaints will be dealt with in accordance with the school's complaints policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

REVIEW

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 2 years. The policy review will be undertaken by the Headteacher or nominated representative.

APPENDIX 1

The Avon Valley School and Performing Arts College

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

- 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, email or fax to the DPO. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO

Subject access requests must be submitted in writing, either by letter, email or fax to the DPO.

Complaints

Complaints about the above procedures should be made to the Chairperson of the Governing Body who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school's complaint procedure.

Complaints which are not appropriate to be dealt with through the school's complaint procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

Contacts

If you have any queries or concerns regarding these policies / procedures then please contact Miss Alison Davies**,** Headteacher.

School Data Protection Officer (DPO) – Warwickshire Education Services (WES)
schooldpo@warwickshire.gov.uk

Further advice and information can be obtained from the Information Commissioner's Office,
www.ico.gov.uk