




**PENK VALLEY
ACADEMY TRUST**

*Learning
Together*

General Data Protection Regulation Policy

Adopted by Trustees:	
Signed:	
Date:	March 2024
This policy is reviewed annually by the Audit and Risk Committee	
Review date:	January 2025



COLLABORATION



CHALLENGE



CURIOSITY



CARE

POLICY INFORMATION

Date of last review:	January 2024	Review period:	Annually
Date ratified by Trustees:	18/03/24	Trustee committee responsible:	Audit and Risk
Policy owner:	Chief Operations Officer	Executive team member responsible:	Chief Operations Officer

Reviews/revisions

Review date	Changes made	By whom
March 2023	New policy.	LMC
January 2024	Updates to DPO and DPL	LMC

Equality and GDPR

All Penk Valley Academy Trust policies should be read in conjunction with our Equal Opportunities and GDPR policies.

Statement of principle – Equality

We will take all possible steps to ensure that this policy does not discriminate, either directly or indirectly against any individual or group of individuals. When compiling, monitoring and reviewing the policy we will consider the likely impact on the promotion of all aspects of equality as described in the Equality Act 2010.

Statement of principle – GDPR

Penk Valley Academy Trust recognises the serious issues that can occur as a consequence in failing to protect an individual adult’s or child’s personal and sensitive data. These include emotional distress, physical safety, child protection, loss of assets, fraud and other criminal acts.

Penk Valley Academy Trust is therefore committed to the protection of all personal and sensitive data for which it holds responsibility as the Data Controller and the handling of such data in line with the data protection principles and the Data Protection Act (DPA)/GDPR.

Penk Valley Academy Trust will be referred to as **PVAT** for the remainder of the document which includes all schools who are members of PVAT, business operations and centralised services.

GENERAL DATA PROTECTION REGULATION POLICY

Contents

1. Aims	
2. Legislation and guidance	
3. Definitions	
4. The Data Controller	
5. Roles and responsibilities	
6. Data protection principles	
7. Collecting personal data	
8. Sharing personal data	
9. Subject access requests and other rights of individuals	
10. Parental requests to see the educational record.....	
11. Photographs and videos	
12. CCTV.....	
13. Biometric data.....	
14. Data protection by design and default	
15. Data security and storage of records	
16. Disposal of records	
17. Personal data breaches	
18. Training	
19. Monitoring arrangements	

1. Aims

PVAT aims to ensure that all personal data collected about staff, pupils, parents, governors, trustees, visitors and other individuals is collected, stored and processed in accordance with the UK GDPR General Data Protection Regulation (GDPR) and the Data protection Act 2018.

This policy applies to all personal data, regardless of format.

2. Legislation and legal framework

This policy meets the requirements of the UK GDPR General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018). It is based on guidance published by the Information Commissioner's Office (ICO).

3. Definitions

Personal data

Any information relating to an identified, or identifiable, individual.

This may include the individual's:

- Name (including initials)
- Identification number
- Location data
- Online identifier, such as a username. It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

Special categories of personal data

Personal data which is more sensitive and so needs more protection, including information about an individual's:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetics
- Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes
- Health – physical or mental
- Sex life or sexual orientation

Processing

Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.

Processing can be automated or manual.

Data subject

The identified or identifiable individual whose personal data is held or processed.

Data Controller

A person or organisation that determines the purposes and the means of processing of personal data.

Data Processor

A person or other body, other than an employee of the Data Controller, who processes personal data on behalf of the Data Controller.

Personal data breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The Data Controller

PVAT processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a Data Controller.

PVAT is registered as a Data Controller with the ICO and will renew this registration annually or as otherwise legally required.

Our registration reference is ZA343630.

5. Roles and responsibilities

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

5.1 Trustees

The Trust Board has overall responsibility for ensuring that PVAT complies with all relevant data protection obligations and approving the measures presented by the Executive team.

5.2 Executive team

Responsible for setting of the strategy, policy making and putting measures in place for the protection of data within PVAT.

5.3 Data Protection Officer

The data protection officer (DPO) is responsible for monitoring our compliance with data protection law, and providing support and guidance as required.

The DPO is also the first point of contact for individuals whose data PVAT processes, and for the ICO.

Contact details

Our DPO is Nicola Cook, SchoolsDPO Ltd and is contactable through the trust/nicola@schoolsdpo.com. Full details of the DPO's responsibilities are set out in the SchoolsDPO service specification.

5.3 Trust Data Protection Lead

The trust data protection lead (DPL) is responsible for overseeing the implementation of this policy, monitoring compliance with data protection law and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the Governing Board and, where relevant, report to the Board their advice and recommendations on PVAT data protection issues.

Contact details

Our DPL is Caroline Harley who is also a first point of contact for individuals whose data PVAT processes. Contactable via DPO@penkvalley.co.uk.

5.4 Headteacher, Staff Managers

The Headteacher acts as the representative of the Data Controller of their school and on a day-to-day basis within their school environment and implements the policy.

5.5 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy.
- Informing PVAT of any changes to their personal data, such as a change of address.

and

Contacting the DPL 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 or 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.

5.6 Local Governing Committee's and volunteers

Subject to the same rules as staff.

6. Data protection principles

The General Data Protection Regulation is based on data protection principles that PVAT 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.

We are also required to be able to demonstrate evidence of our compliance with the GDPR under the principle of accountability.

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

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We 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 PVAT can fulfil a contract with the individual, or the individual has asked PVAT to take specific steps before entering a contract.
- The data needs to be processed so that PVAT 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 PVAT 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 PVAT 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 General Data Protection Regulation and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on legitimate interest as a basis for processing.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by Data Protection Law. This will normally be through our privacy notices.

7.2 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 need the personal data they hold, it will be handled within the timeframe laid out in the data retention schedule.

8. 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.

We will also share personal data with law enforcement and Government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud.
- The apprehension or prosecution of offenders.
- The assessment or collection of tax owed to HMRC.
- In connection with legal proceedings.
- Where the disclosure is required to satisfy our safeguarding obligations.
- Research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the United Kingdom, we will do so in accordance with Data Protection Law and undertake a risk assessment.

9. Subject Access Requests and other rights of individuals

9.1 Subject Access Requests

Individuals have a right to make a 'Subject Access Request' to gain access to personal information that PVAT 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 can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing to the DPL and 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 DPL.

9.2 Children and Subject Access Requests

Personal data about a child belongs to that of the child. For a parent or Carer to make a Subject Access Request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a Subject Access Request. This however is only a guide and the pupil's ability to understand their rights will always be judged on a case-by-case basis.

For children over the age of 12 we will require evidence that parents can have the right to see the data, this can be through email, letter or in person. See point 10 regarding accessing the pupil's educational record.

9.3 Responding to Subject Access Requests

When responding to requests, we:

- May ask the individual to provide two forms of identification.
- May contact the individual via phone to confirm the request was made.
- Will respond without delay and within one month of receipt of the request.
- Will provide the information free of charge.
- May tell the individual we will comply within three months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month and explain why the extension is necessary.

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests.
- Is contained in adoption or parental order records.
- Is given to a court in proceedings concerning the child.

- If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which considers administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.4 Other data protection rights of the individual

In addition to the right to make a Subject Access Request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- 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 based on public interest.
- Request a copy of agreements under which their personal data is transferred outside of the United Kingdom.
- 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.
- 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 DPL. If staff receive such a request, they must immediately forward it to the DPL.

10. Parental requests to see the educational record vs Subject Access Requests

As a parent you may have access to the pupils educational record, outside of this record, all other information will be subject to a Subject access request. Being an academy the legislation for the educational record falls under the same legislation for subject access, therefore data will be provided within 1 calendar month.

When deciding whether to view the education record, or to submit a full Subject Access Request it is worth considering what information you wish to obtain.

If you submit a request to view or receive a copy of the education record, PVAT will only disclose the information contained in the record and are not obliged to disclose any further personal data that it may hold. This is likely to be swifter than a full Subject Access Request.

If you submit a Subject Access Request to the school or PVAT directly for all your, or your child's personal data, it is likely to disclose both information contained in the education record and any other personal data the organisation may hold.

When it may be withheld

There are certain circumstances where an education record may be withheld; for example, where the information might cause serious harm to the physical or mental health of the pupil or another individual.

The request for access would also be denied if it would mean releasing examination marks before they are officially announced.

11. Photographs and videos

As part of PVAT activities, we may take photographs and record images of individuals.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

- Within PVAT on notice boards, in PVAT magazines, brochures and newsletters, etc.
- Outside PVAT by external agencies such as the PVAT photographer, newspapers and campaigns.
- Online on PVAT's websites.
- LinkedIn, Facebook, X, YouTube and Instagram are our formal online profiles. There are profiles for each school including PVAT.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further. Images online will be subject to the removal process and the timeframe of the hosting company.

Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the General Data Protection Regulation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or pupils where appropriate) have agreed to this.

12. CCTV

12.1

- PVAT understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

12.2

- PVAT notifies all pupils, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and signage.

12.3

- Cameras are only placed where they are necessary to fulfil their purpose.

12.4

- All CCTV footage will be kept for 28 days; the ICT team are responsible for ensuring a system able to record and that the records are secure.

12.5

- Headteachers are responsible for ensuring access to the data is recorded and CCTV is used within PVAT for the following purposes of:
 - Deter/detect bullying.
 - Deter/detect crime, theft and vandalism.

- To ensure compliance with code of behaviours.
- To aid security.
- For accident investigation and verification.
- To enable the school to discharge its duty of care.

13. Biometric data

PVAT does not use biometric data, therefore, we hold no biometric data.

14. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge.
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant Data Protection Law (see section 6).
- Completing data protection impact assessments where PVAT's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process).
- Integrating data protection into internal documents including this policy, any related policies and Privacy Notices.
- Regularly training members of staff on Data Protection Law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance.
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant.
- Appropriate safeguards being put in place if we transfer any personal data outside of the United Kingdom (UK), where different data protection laws will apply.

Maintaining records of our processing activities, including:

- For the benefit of data subjects, making available the contact details of our DPO and all information we are required to share about how we use and process their personal data (via our Privacy Notices).
- For all personal data that we hold, maintaining an internal record of the type of data, Data Subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, how and why we are storing the data, retention periods and how we are keeping the data secure.

15. Data security and storage of records

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.

In particular:

- 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/display boards, or left anywhere else where there is general access.
- Passwords that are complex using three unconnected words at least 8 characters long containing numbers and special characters are used to access PVAT computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices.
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for PVAT-owned equipment (see our Cyber Security Policy and Acceptable Use Agreement <https://forms.office.com/e/6bDEtVtZiV>)
- 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 (see section 8).

16. Disposal of records

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 PVAT's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with Data Protection Law.

17. Personal data breaches

PVAT will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out by the ICO. When appropriate, we will report the data breach to the ICO within 72 hours.

18. Training

All staff and governors are provided with data protection training and cyber security training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or PVAT's processes make it necessary.

19. Monitoring arrangements

The DPL is responsible for monitoring and reviewing this policy and will be reviewed yearly or when significant legislation changes happen.