PASTways

 Date Created: 1st September 2025

 Review Date: 1st September 2026

 Signed:

Data Protection Act

Contents

[Aims 3](#_Toc202784989)

[Legislation and guidance 3](#_Toc202784990)

[Definitions 4](#_Toc202784991)

[Roles and Responsibilities 5](#_Toc202784992)

[Data Protection Officer (DPO) 5](#_Toc202784993)

[The Manager 5](#_Toc202784994)

[All Staff 5](#_Toc202784995)

[Data Protection Principles 5](#_Toc202784996)

[Collecting Personal Data 6](#_Toc202784997)

[Lawfulness and Transparency 6](#_Toc202784998)

[Limitations and Accuracy of Collection 7](#_Toc202784999)

[Sharing Data 7](#_Toc202785000)

[Subject Access Requests and Other Rights 8](#_Toc202785001)

[Subject Access Requests 8](#_Toc202785002)

[Children and Subject Access Requests 8](#_Toc202785003)

[Responding to Subject Access Requests 9](#_Toc202785004)

[Other Rights of the Individual 9](#_Toc202785005)

[CCTV 10](#_Toc202785006)

[Photography and videos 10](#_Toc202785007)

[Integrated Data Protection 10](#_Toc202785008)

### Aims

PASTways endeavours to ensure that all personal data collected regarding students, staff, visitors, volunteers, trustees, and other individuals entering the environment is collected, stored, and processed in accordance with UK data protection legislation.

This protocol applies uniformly to all data, irrespective of whether it is in physical or electronic form.

### Legislation and guidance

This policy meets the requirements of

* UK General Data Protection Regulation (UK GDPR) <https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>

This policy is guided by The Information Commissioner Office (ICO)

* Guidance on GDPR <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/>
* Code of practice for the use of CCTV <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/881538/SCC___ICO_DPIA_guidance_V3_FINAL_PDF.pdf>

PASTways does not use any biometric data.

## Definitions

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Personal Data | Information related to an identified or identifiable living person. Such as:* Name
* Address
* Identification numbers (NI number, Passport number, etc)
* Location data
* Photos and/or video footage
* Online identifiers (usernames)
 |
| Special Categories of Personal Data | This is sensitive personal data and requires more protection; this is information such as:* Racial or ethnic background
* Genetics
* Mental and physical health
* Political opinions
* Religious beliefs
* Trade union membership
* Sexual orientation and sex life
 |
| **Processing**  | Anything that is done to personal data, either manually or electronically. Such as:* Collecting
* Storing
* Organising
* Altering/adapting
* Using
* Retrieving
* Destroying
* Erasing
 |
| **Data Subject**  | The individual (identified or identifiable) whose personal data is processed and/or held |
| **Data Controller** | The person or organisation deciding the means and purpose of processing personal data. |
| **Data Processor**  | Processes personal data on behalf of the data controller. |
| **Personal Data Breach** | A breach of security leading to accidental and/or unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data. |
| **Data Protection Officer (DPO)** | A named individual who helps PASTways protect their data and stay compliant and up to date with regulations |
| **Information Commissioner’s Office (ICO)** | UK supervisory authority with the responsibility for enforcing the data protection rules and regulations (GDPR) |
| **GDPR** | General Data Protection Regulations |

## Roles and Responsibilities

This policy applies to all staff and volunteers at PASTways.

## Data Protection Officer (DPO)

The DPO is responsible for monitoring PASTways' compliance with data protection law, overseeing the implementation of this policy, and developing related guidelines and policies where appropriate.

They will report to the trustees and the manager with advice and recommendations on data protection issues.

The DPO is the first point of contact for the ICO, and the full responsibilities of the DPO will be set out in their contract.

The DPO is Jade Belcher; the DPO and manager are responsible for day-to-day data protection matters at PASTways.

The DPO is responsible for monitoring and reviewing this policy annually, or more frequently if necessary.

## The Manager

The manager at PASTways will act as the data controller on a daily basis.

## All Staff

All staff are responsible for:

* Collecting, storing and processing any personal data per this policy
* Making PASTways aware of any changes to their data, e.g., a change in address
* Contacting the DPO in these circumstances:
	+ Any questions about this policy, GDPR, retaining and keeping personal data secure.
	+ Any concerns that this policy is not being followed
	+ If there has been a data breach
	+ Deal with data protection rights invoked by an individual
	+ When engaging in a new activity that could affect the privacy of individuals
	+ If they need help drafting a contract and/or sharing data

### Data Protection Principles

PASTways must comply with the data protection principles on which the UK GDPR is based. This policy outlines how PASTways aims to adhere to these principles.

These principles state that personal data must be:

* Processed fairly, lawfully and transparently
* Collected for legitimate, specified and explicit reasons
* 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 necessary, and for which it was processed
* Processed in a way that ensures it is completely secure

## Collecting Personal Data

### Lawfulness and Transparency

PASTways will only process personal data where we have at least one of 6 lawful bases to do so under data protection law.

* The data must be processed to fulfil a contract with the individual, or the individual has asked PASTways to take specific steps before entering a contract.
* Data needs to be processed to comply with legal obligations
* Data needs to be processed to ensure the vital interests of the individual or another person, e.g., to protect life
* Data needs to be processed for PASTways to perform a task in the public interest.
* Data needs to be processed for the legitimate interests of Past way, or a third party, providing the individual's rights and freedoms are not overridden
* The individual (or their parent/guardian, where appropriate) has given explicit consent

For special categories of personal data, PASTways will also meet one of the special category conditions for processing data:

* The individual (or their parent/guardian, where appropriate) has given explicit consent
* Data needs to be processed to ensure the vital interests of the individual or another person, e.g., to protect life
* The data has been made manifestly public by the individual
* Data needs to be processed to exercise rights or obligations about employment, social security or social protection law
* Data needs to be processed for the establishment or defence of legal claims
* Data needs to be processed for health or social care purposes and/or public health reasons. The processing is done by, or under direction from, a health or social work professional

PASTways will meet conditions set out under data protection law for criminal defence data. These include:

* The individual (or their parent/guardian where appropriate) has given explicit consent
* Data needs to be processed to ensure the vital interests of the individual or another person, e.g., to protect life
* The data has been made manifestly public by the individual
* Data needs to be processed in connection with or for legal proceedings, to obtain legal advice or for the establishment or defence of legal rights
* Data needs to be processed for reasons of substantial public interest.

Wherever we collect personal data directly from individuals, PASTways will provide them with relevant information as data protection law requires.

PASTways will always consider the fairness of data processing; we will not handle personal data in ways an individual would not reasonably expect or use personal data in ways that will have unjustified adverse effects on the individual.

### Limitations and Accuracy of Collection

Data will only be collected for specific, explicit and legitimate reasons. We will aim to explain these reasons to individual when we first collect their data.

If we wish to use personal data for reasons other than first stated to the individual, we will inform the individual of how we do not want to use data and seek consent where necessary.

## Sharing Data

PASTways will not typically share data without the individual's consent. However, there are certain circumstances where we may be required to share data without prior permission. Situations include but are not limited to:

* Issues with parents/carers/students that put the safety of staff at risk
* The need to liaise with other agencies – where necessary, we will gain consent before this
* Suppliers/contractors need data to be able to provide a service to staff and/or students, e.g., IT companies; when doing this, we will:
	+ Only appoint suppliers/contractors that provide sufficient guarantees that they comply with data protection law
	+ Establish a contract with the contractor/supplier to ensure the fair, lawful processing of data
	+ Only share data that the supplier/contractor needs to carry out their services
* PASTways will share personal data with law enforcement and government bodies where legally required to do so
* We may need to share personal data with emergency services and local authorities to help them respond to emergencies that affect students and staff

## Subject Access Requests and Other Rights

### Subject Access Requests

Individuals have the right to make a Subject Access Request to gain access to personal information PASTways holds about them. This includes:

* Confirmation that their data is being processed
* The purposes of data processing
* Access to a copy of the data
* Categories of personal data concerned
* With Who the data has been/will be shared
* How long will the data be stored for
* The right to request rectification, erasure or restriction of data processing
* The right to complain to supervisory bodies
* The source of the data
* The safeguards when transferring data

Subject access requests can be submitted in any form but can be responded to faster if they are made in writing and include the following:

* individual's name
* Correspondence address
* Contact number
* Email address
* Details of the information requested

If staff receive a Subject Access Request, they must immediately forward it to the DPO.

### Children and Subject Access Requests

The personal data of children belongs to the child, not the parent or carer. For a parent/carer to submit a Subject Access Request concerning their child, the child must have either:

* Given explicit consent
* Be unable to understand the rights and implications of submitting a Subject Access Request

Children over 12 years old are generally considered capable of understanding the rights and implications of submitting a Subject Access Request. However, this is not a rule, and a student’s ability to understand their rights will always be judged on a case-by-case basis.

###  Responding to Subject Access Requests

When responding to requests, PASTways may:

* Ask the individual to produce two forms of identification
* Contact an individual by phone to confirm the request
* Tell the individual we will comply within three months of receipt of the request, where the request is complex and/or numerous. We will inform the individual of this and explain why the period is three months

When responding to request, PASTways will:

* Respond without delay and aim to complete within one month from all receipt of the request (or receipt of additional data where applicable)
* Provide the information free of charge.

PASTways may not disclose information for multiple reasons, such as:

* Potential for serious harm to the physical and/or mental health of the student or another individual
* Would reveal the student has been/is being abused or is at risk of abuse, where knowledge of this information would not be in the student’s best interests
* Would include the personal data of another that is not anonymised, and we do not have their consent
* Is part of certain sensitive documents, such as
	+ Exam scripts
	+ Related to crime
	+ Related to immigration
	+ Related to legal proceedings
	+ Management forecasts
	+ Negotiations
	+ Confidential references

If a request is unfounded or deemed excessive, PASTways may refuse to act on it or charge a reasonable fee. We will consider whether the request is repetitive when making this decision.

When a request is refused, we will inform the individual of the reason. They have the right to complain to a supervisory body if they wish, or they can seek to enforce their Subject Access Request through the courts.

### Other Rights of the Individual

In addition to submitting a Subject Access Request, individuals also have the right to:

* Withdraw consent from data processing at any time
* Ask PASTways to rectify, erase or restrict the processing of their data (in certain circumstances)
* Object to processing justified based on public or legitimate interests or official authority
* Be notified of a data breach (in certain circumstances)
* Make a complaint to a supervisory body

Individuals should submit their request to the DPO. If staff receive a request, they should forward it to the DPO.

### CCTV

We use CCTV in various locations throughout the building to ensure safety at PASTways. We do not need to ask for permission from individuals to use CCTV, but we make clear where recordings are being made and ensure security cameras are visible with prominent ‘CCTV in use’ signage. Any enquiries about the use of CCTV should be directed to the manager.

### Photography and videos

* As part of PASTways activities, we may take photographs or videos of individuals. We will obtain consent from both the parent/guardian and the student when using photos or videos of individuals for communications, marketing, and/or promotional materials. Uses may include:
* • Within the school
* • Online on the PASTways website
* • Outside of PASTways, such as newspapers or campaigns.

### Integrated Data Protection

* PASTways has taken steps to show how we have embedded data protection into all our data processing activities. These include:
* • Appointing a suitable DPO, ensuring they have the resources and training to perform their duties effectively
* • Processing only personal data that is necessary and for a specific purpose
* • Incorporating data protection into internal documents
* • Regularly reviewing policies and practices to ensure compliance
* • Implementing appropriate safeguards when transferring data
* • Providing staff with training on data protection

Signed 

Manager Dated …01/09/2025