PWL PATHWAYS LDN
Employment, Skills & Training

Data Protection and GDPR Policy

Version 8.0

Contents

Version Control

Version	Reviewer Name	Date	Next Review	Comments
1.0	Rena Panesar	Jan 2018	Jan 2019	First Policy.
2.0	Rena Panesar	Jan 2019	Jan 2020	Updated
3.0	Rena Panesar	Jan 2020	Jan 2021	Updated
4.0	Rena Panesar	Jan 2021	Jan 2022	Updated
5.0	Rena Panesar	Jan 2022	Jan 2023	Updated
6.0	Rena Panesar	Jan 2023	Jan 2024	Updated
7.0	Paul Tumwine	Jan 2024	Jan 2025	Updated.
8.0	Policy Pros	Oct 2025	Oct 2026	Retemplated and updated.

Who We Are

We are a UK-registered Limited Company:

- **Name: PATHWAY'S LDN LTD**
- **Company number: 10239394.**
- **Registered Address: Belmont Building, Belmont Road, Uxbridge, Greater London, England, UB8 1HE**
- **Information Commissioner's Office registration number: ZA804254**

Introduction

Pathways LDN is committed to protecting the privacy and rights of everyone whose personal data we process, including data relating to our staff, learners, employers, partners, etc.

We recognise that the personal data entrusted to us must be handled lawfully, fairly, and transparently in line with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. This policy sets out our approach to data protection and explains how we safeguard information, uphold individual rights, and ensure compliance with relevant legislation.

Our aim is to ensure that all staff, contractors, and partners understand their responsibilities in relation to data protection and that all of our stakeholders can have confidence that their information is processed securely and responsibly.

Who and What This Policy Applies To

This policy applies to all those working for or on behalf of Pathways LDN (who are referred to as staff or staff members throughout) and to any personal (or sensitive personal) information and criminal records information processed by Pathways LDN.

Policy Support

If you have any questions or comments about the content of this policy or if you need further information, please contact our Directors by email at paul@pathwaysldnltd.com or rena@pathwaysldnltd.com or by telephone at 07508114160 or 07982906672.

Definitions

Data Subject
Means the individual to whom the personal information relates.

Personal Information
Sometimes known as personal data means information relating to an individual who can be identified (directly or indirectly) from that information.

Processing Information
Means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or otherwise using or doing anything with it.

Controller
A controller is a natural or legal person, public authority, agency, or any other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Processor
The UK GDPR defines a processor as a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Pseudonymised
This is the process by which personal information (or sensitive personal information) is processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to technical and organisational measures to ensure that the personal information cannot be attributed to an identifiable individual.

Sensitive Personal Information
Sometimes known as 'special categories of personal data' or 'sensitive personal data', means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

Policy

Data Protection Principles

Pathways LDN endorses fully and adheres to the Data Protection Principles listed below. When processing data, we will ensure that it is:

- ✔ processed lawfully, fairly and in a transparent way
- ✔ processed no further than the legitimate purposes for which that data was collected
- ✔ limited to what is necessary in relation to the purpose
- ✔ accurate and kept up-to-date
- ✔ kept in a form which permits identification of the data subject for no longer than is necessary
- ✔ processed in a manner that ensures the security of that personal data and protects against unauthorised or unlawful processing and accidental loss, destruction, or damage
- ✔ processed by a controller who can demonstrate compliance with the principles

These principles must be observed at all times when processing or using personal information.

The Basis for Processing Personal Information

Concerning any processing activity, we will, before the processing starts for the first time, and then regularly while it continues:

- Review the purposes of the processing activity and select the most appropriate lawful basis (or bases) for that processing, for example:
    - That the data subject has consented to the processing;
    - That the processing is necessary for the performance of a contract to which the data subject is a party;
    - To take steps at the request of the data subject before entering into a contract;

  - That the processing is necessary for compliance with a legal obligation to which Pathways LDN is subject;
  - That the processing is necessary for the protection of the vital interests of the data subject or another natural person;
  - That the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority; or
  - That the processing is necessary for the legitimate interests of Pathways LDN or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the Data Subject.
- Document our decision as to which lawful basis applies to help demonstrate our compliance with the data protection principles.
- Include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s).
- Where criminal offence information is processed, also identify a lawful condition for processing that information and document it.
- If processing is based on legitimate interests, determine whether Pathways LDN's legitimate interests are the most appropriate basis for lawful processing, and:
  - Conduct a Legitimate Interest Assessment (LIA) and keep a record of it to ensure that we can justify our decision;
  - If the LIA identifies a significant privacy impact, consider whether we also need to conduct a data protection impact assessment (DPIA);
  - Keep the LIA under review and repeat it if circumstances change; and
  - Include information about our legitimate interests in our relevant privacy notice(s).

Sensitive Personal Information

Pathways LDN may need to process sensitive personal information. We will only process sensitive personal information if:

- We have a lawful basis for doing so set out above; and
- One of the special conditions for processing sensitive personal information applies, for example:

- The data subject has given explicit consent so that Pathways LDN can provide its services.
- The processing is necessary for exercising the employment law rights or obligations of Pathways LDN or the data subject.
- The processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent.
- The processing relates to personal data, which is manifestly made public by the data subject.
- The processing is necessary for the establishment, exercise, or defence of legal claims; or
- The processing is necessary for reasons of substantial public interest.

- The individual has been properly informed of the nature of the processing, the purposes for which it is being carried out, and the legal basis for it.

Criminal Records Information – Staff

Pathways LDN may process criminal records data (also referred to as "criminal conviction data" or "Disclosure and Barring Service (DBS) data") in limited circumstances where it is necessary and lawful to do so. This typically applies to roles where employees or self-employed colleagues (e.g., tutors or careers advisors) have direct contact with our learners (many of whom are under 18 or may be vulnerable), in line with our safeguarding obligations.

Criminal records data will only be processed:

- Where a legal basis exists under Article 6 and a condition under Article 10 of the UK GDPR is met
- In accordance with Schedule 1 of the Data Protection Act 2018 (e.g., for reasons of substantial public interest, such as safeguarding)
- Following a risk-assessed and proportionate approach

Access to criminal records data is strictly limited to those with a legitimate need to know, and the data is stored securely in accordance with our retention and security protocols. We ensure that the data is handled sensitively and in full compliance with relevant data protection legislation and guidance.

Pathways LDN will never retain criminal records information for longer than necessary and will not use it for purposes beyond verifying suitability for work requiring such vetting.

Documentation and Records

We will keep records of processing activities, including:

- A description of the categories of individuals and categories of personal data;
- Categories of recipients of personal data;
- The purposes of the processing;
- Where relevant, details of transfers to third countries, including documentation of the transfer mechanism safeguards in place;
- Where possible, retention schedules; and
- Where possible, a description of technical and organisational security measures.

As part of our record of processing activities, we document, or link to documentation, on:

- Records of consent.
- Controller-processor contracts.
- The location of personal information.
- DPIAs (if relevant); and
- Records of data breaches.

If we process sensitive personal information or criminal records information, we will keep written records of:

- The relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose;
- The lawful basis for our processing; and
- Whether we retain and erase the personal information following our policy document, and if not, the reasons for not following our policy.

We will regularly review the personal information we process and update our documentation accordingly. This may include:

- Carrying out information audits to find out what personal information Pathways LDN holds and how we process it.

- Reviewing our policies, procedures, contracts, and agreements to address areas such as retention, security, and data sharing.

Data Protection Impact Assessments (DPIAs)

Before any new form of technology is introduced, and where data processing is likely to result in a high risk to an individual's data protection rights, we will, before commencing the processing, carry out a DPIA to assess:

- Whether the processing is necessary and proportionate concerning its purpose.
- The risks to individuals.
- What measures can be put in place to address those risks.

Privacy Notices

Pathways LDN will issue privacy notices from time to time, informing data subjects about the personal information that we 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.

Individual Rights

Data subjects (staff, learners, their parents/guardians, the guardians, anyone who has been referred to us, etc.) have the following rights concerning their personal information:

- The right to access personal data held about them (making a subject access request);
- The right to be informed about how and why their data is used;
- The rights to have their data rectified, erased or restricted;
- The right to object;
- The right to portability of their data; and
- The right not to be subject to a decision based solely on automated processing.

To exercise any of these rights, the data subject should contact the Directors (their contact details can be found in the Policy Support section at the top of this policy).

However, some exemptions and restrictions can, in some circumstances, be legitimately applied to exempt or qualify the right of individuals to exercise their rights. For example:

- If fulfilling the request would undermine the prevention, investigation, detection, or prosecution of criminal offences.
- If the processing of personal data is necessary for the establishment, exercise, or defence of legal claims.
- If fulfilling them would infringe upon the rights and freedoms of others, including trade secrets or intellectual property.

Staff Member Obligations

All staff members of Pathways LDN have a fundamental responsibility to ensure the protection of personal data processed by us.

Specifically, all staff members must:

- Familiarise themselves with this Data Protection and GDPR Policy and any associated guidelines or procedures. Reading and understanding this policy and any updates/addenda form part of our mandatory training.
- Only process personal data for legitimate business purposes as instructed by us and in a manner that is fair, transparent, and compliant with UK GDPR principles.
- Only collect, access, or use the minimum amount of personal data necessary for the specific task or purpose. Avoid collecting or holding data that is not directly relevant or required. Never attempt to access personal data that they do not have a legitimate business need or authorisation to view.
- Take reasonable steps to ensure that the personal data they handle is accurate, complete, and kept up-to-date.
- Keep all personal data secure and confidential, whether in physical or digital format.
- Immediately report any suspected or actual personal data breach (as set out below).
- Dispose of personal data securely when it is no longer required (e.g., shredding paper documents and securely deleting electronic files).

Information Security

Pathways LDN will use appropriate technical and organisational measures to keep personal information secure and to protect against unauthorised or unlawful processing and accidental loss, destruction, or damage. For example, all company devices and software platforms are password-protected, and access is granted on a role-specific, need-to-know basis to ensure that only authorised colleagues can view or process personal information relevant to their responsibilities.

In rare cases where Pathways LDN uses third parties to process personal information on its behalf or where third parties may have access to personal information (e.g. our website developers), additional security arrangements will be implemented in contracts with those organisations to safeguard the security of personal information. In particular, contracts with external organisations will provide that:

- The organisation may act only on the written instructions of Pathways LDN;
- Those processing the data are subject to a duty of confidence;
- Appropriate measures are taken to ensure the security of processing;
- Sub-contractors are only engaged with the prior consent of Pathways LDN and under a written contract;
- The organisation will assist Pathways LDN in providing subject access and allowing individuals to exercise their rights under the GDPR;
- The organisation will assist Pathways LDN in meeting its GDPR obligations concerning the security of processing, the notification of data breaches and data protection impact assessments;
- The organisation will delete or return all personal information to Pathways LDN as requested at the end of the contract; and
- The organisation will submit to audits and inspections and provide Pathways LDN with whatever information it needs to ensure that they are meeting its data protection obligations.

Please see our Information Security Policy for further information.

Storage and Retention of Personal Information

Personal information (and sensitive personal information) will be kept securely following Pathways LDN's principles below:

- Personal information (and sensitive personal information) should not be retained any longer than necessary. The length of time that data should be retained will depend upon the circumstances, including the reasons why the personal information was obtained.
- Personal information (and sensitive personal information) that is no longer required will be deleted permanently from our information systems, and any hard copies will be destroyed securely (shredded).

Data Breaches

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

When a staff member becomes aware of a suspected or actual data breach, they must report it immediately to the Directors so that appropriate action can be taken in line with Pathways LDN's Data Breach Response Procedure (below).

In the event of a Data Breach, Pathways LDN will:

- Immediately take such steps as are necessary to minimise the risk to the data subjects affected and the organisation.

- Assess the situation and determine what further steps need to be taken to minimise harm.
- As required, make the required report of a data breach to the Information Commissioner's Office without undue delay.
- Notify the affected data subjects if a data breach is likely to result in a high risk to their rights and freedoms, and notification is required by law.
- Take steps as necessary to ensure that similar breaches cannot happen again.

International Transfer of Data

Whilst Pathways LDN does not intend to transfer personal information outside the European Economic Area (EEA), our website and some of the software used by Pathways LDN may be hosted outside of the EEA.

However, we have determined that this data is secure on the basis that the country, territory or organisation is designated as having an adequate level of protection and has provided adequate safeguards by way of acceptable data protection clauses.

Selling Data

At Pathways LDN, we are committed to upholding the highest standards of data protection and privacy and want to assure all individuals that we will never sell or trade personal data to any third parties.

Managing Subject Access Requests

Data subjects have the right to access any personal data that is being kept about them by Pathways LDN. To do this, the data subject must make a 'subject access request'.

To make a subject access request, the data subject should contact the Directors (their contact details can be found in the Policy Support section at the top of this policy).

Pathways LDN aims to deal with the subject access request as quickly as possible, and all requests will be completed within 30 days unless defined as complex. If the time exceeds 30 days, the requester will be notified in writing.

Subject Access Requests coming directly from the data subject will be free. However, we can charge a fee if requests become unfounded or excessive.

Alternatively, we can refuse to comply with the request, for example, if the request is manifestly unfounded or manifestly excessive.

Please Note:

- Some of the rights under the GDPR may be limited where we have an overriding interest or legal obligation to continue to process the data, or where data may be exempt from disclosure by law.
- We sometimes need to request specific information from a requester to help us confirm their identity and ensure their right to access the information (or to exercise any of their other rights). This is an appropriate security measure to ensure that personal information is not disclosed to anyone without the right to receive it.

Non-Compliance

Pathways LDN takes compliance with this policy very seriously. Failure to comply with the policy:

- Puts data subjects at risk.
- Carries the risk of significant civil and criminal sanctions for the individual and Pathways LDN.
- May, in some circumstances, amount to a criminal offence by the individual.

Because of the importance of this policy, a staff member's failure to comply will usually be treated as gross misconduct and will result in their working agreement/contract being terminated without notice.

Reviewing

Pathways LDN Ltd. is committed to ensuring our policies are effective and up-to-date.

The Directors are responsible for this process and will review this policy at least once a year or more frequently if needed due to changes in laws, regulatory guidance, or best practice.

This policy will be made available in other formats upon request, and all learners are encouraged to speak to any member of staff if they have any questions or require clarification.