POSITIVE PATHWAYS
RESIDENTIAL CARE SERVICES FOR CHILDREN & YOUNG PEOPLE

DATA PROTECTION POLICY

Reviewed & updated:	February 2026

Frame of Reference and Standards

This policy has been developed with respect to:

- The Children's Homes Regulations and Standards (April) 2015
- Data Protection Act 1998
- GDPR Regulations (25th May 2018)
- Equality Act 2010

Introduction

Positive Pathways Limited (the 'Company') needs to collect and use certain types of information about the Individuals or Service Users who come into contact with the Company in order to carry on its work. For example, employees are required to provide their home address and telephone number for the purposes of correspondence. Similarly, information about Disclosure and Barring Service (DBS) checks is collected and securely stored as part of the Company recruitment policy in order to comply with statutory guidelines. The Company has a responsibility under the Data Protection Act 1998 and the General Data Protection Regulations (GDPR) (25th May 2018) to ensure that this personal information is collected and dealt with appropriately, whether it is collected on paper, stored in a computer database, or recorded on other material. The Company strives to comply with the six principles enshrined in the GDPR, specifically:

1. Lawfulness, fairness, and transparency
2. Purpose limitation
3. Data minimization
4. Accuracy
5. Age limitation
6. Integrity and confidentiality

Data Controller

Positive Pathways is the Data Controller under the Act, which means that it determines what personal information will be held and what it will be used for. It is also responsible for notifying the Information Commissioner's Office (ICO) of the types of data it holds or is likely to hold, and the general purposes that the data will be used for.

Disclosure

Positive Pathways may be required to share certain types of share data with other agencies such as Local Authorities and funding bodies. The

Individual/Service User will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows Positive Pathways to disclose data (including sensitive data) without the data subject's consent, as follows:

1. Undertaking a legal duty or as authorised by the Secretary of State.

2. Protecting vital interests of an Individual/Service User or other person.

3. The Individual/Service User has already made the information public.

4. Conducting any legal proceedings, obtaining legal advice or defending any legal rights.

5. Monitoring for equal opportunities purposes, e.g. race, disability or religion.

6. Providing a confidential service where the Individual/Service User's consent cannot be obtained or where it is reasonable to proceed without consent, e.g. where it is desirable to avoid forcing stressed or ill Individuals/Service Users to provide consent signatures.

Positive Pathways regards the lawful and correct treatment of personal information as very important to successful working and to maintaining the confidence of those with whom we deal. The Company therefore intends to ensure that personal information is treated lawfully and correctly. To this end Positive Pathways will adhere to the principles of Data Protection, as detailed in the Data Protection Act 1998. Specifically, the principles require that personal information will be:

1. Processed fairly and lawfully and, in particular, will not be processed unless specific conditions are met.

2. Obtained only for one or more of the purposes specified in the Act and not be processed in any manner incompatible with that purpose or those purposes.

3. Adequate, relevant, and not excessive in relation to those purpose(s).

4. Accurate and, where necessary, kept up to date.

5. Not kept longer than is legally required or necessary.

6. Processed in accordance with the rights of data subjects under the Act.

7. Kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information.

8. Not transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate

level of protection for the rights and freedoms of Individuals/Service Users in relation to the processing of personal information.

Through appropriate management and strict application of criteria and controls Positive Pathways will:

- Observe fully the conditions regarding the fair collection and use of information.
- Meet its legal obligations to specify the purposes for which information is used.
- Collect and process appropriate information and only to the extent that it is needed to fulfill its operational needs, or to comply with any legal requirements.
- Ensure the quality of information used.
- Ensure that the rights of people about whom information is held can be fully exercised under the Act. These include:
    - The right to be informed that processing is being undertaken.
    - The right of access to one's personal information where legally permissible.
    - The right to prevent processing in certain circumstances.
    - The right to correct, rectify, block or erase information which is regarded as wrong information.
- Take appropriate technical and organisational security measures to safeguard personal information.
- Ensure that personal information is not transferred abroad without suitable safeguards.
- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information.
- Set out clear procedures for responding to requests for information.

Data Collection

Informed consent is when:

- An Individual/Service User clearly understands why information is needed, who it will be shared with, and the possible consequences of agreeing or refusing the proposed use of the data; and
- Gives their consent.

Positive Pathways will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form. When collecting data the Company will ensure that the Individual/Service User:

1. Clearly understands why the information is needed.

2. Understands what the information will be used for and what the consequences are should the Individual/Service User decide not to give consent to processing.

3. As far as reasonably possible, grants explicit consent, either written or verbal, for data to be processed.

4. Is, as far as reasonably practicable, sufficiently competent to give consent and has given so freely without any duress.

5. Has received sufficient information on why their data is needed and how it will be used.

Data Storage

Information and records relating to Individuals/Service Users will be stored securely and will only be accessible to authorised members of staff. Information will be stored for only as long as it is needed or legally required and will be disposed of appropriately. It is the responsibility of the Company to ensure that all personal and company data is non-recoverable from any computer system previously used within the organisation which has been passed on/sold to a third party.

Data Access and Accuracy

All Individuals/Service Users have the right to access the information that the Company holds about them. The Company will also take reasonable steps to ensure that information is kept up-to-date by asking data subjects whether there have been any changes. In addition**,** the Company will ensure that:

- It has a Data Protection Officer with specific responsibility for ensuring compliance with Data Protection.

- Everyone processing personal information understands that they are contractually responsible for following good data protection practice.

- Everyone processing personal information is appropriately supervised.

- Anybody wanting to make enquiries about handling personal information knows what to do.

- It deals promptly and courteously with any enquiries about handling personal information.

- It describes clearly how it handles personal information.

- It will regularly review and audit the ways it hold, manages, and uses personal information.

- It regularly assesses and evaluates its methods and performance in relation to handling personal information.

- All staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them.

This policy will be updated as necessary to reflect best practice in data management, security, and control and to ensure compliance with any changes or amendments made to the Data Protection Act 1998. In case of any queries or questions in relation to this policy please contact the relevant Line Manager.

Glossary of Terms

Data Controller – The name of the organisation that determines what personal information will be held, how it will be held, and what it will be used for.

Data Protection Act 1998 – The UK legislation that provides a framework for responsible behaviour by those using personal information.

Data Protection Officer – The person(s) responsible for ensuring that the Data Controller follows its data protection policy and complies with the Data Protection Act 1998 and GDPR.

Individual/Service User – The person whose personal information is being held or processed by the Data Controller (e.g. service users, employees, volunteers, trainees, students).

Explicit Consent – is a specific informed agreement that is freely given by an Individual/Service User for the purposes of processing of personal information about her/him. Explicit consent is needed for processing sensitive data.

Notification – Notifying the ICO (www.ico.gov.uk) about the data processing activities of the Company, as certain activities may be exempt from notification.

Information Commissioner – The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 1998.

Processing – means collecting, amending, handling, storing or disclosing personal information.

Personal Information – Information about living individuals that enables them to be identified – e.g. name and address. It does not apply to information about organisations, companies and agencies but applies to

named persons, such as individual volunteers or employees within the Company.

Sensitive Data – refers to data relating to:

- Religion or similar beliefs
- Racial or ethnic origin
- Political affiliations
- Trade union membership
- Physical or mental health
- Sexuality
- Criminal record or proceedings

Positive Pathways Ltd: Data Protection Policy

Employee Consent Form

I confirm that I have read and understood the Company Data Protection Policy.

Name:……

Signed:……

Job title:……

Date:……

Completed copy to:

Supervision file
Personnel file at Head Office