DATA PROTECTION & RETENTION POLICY

November 2019
Version 2
No substantive changes

Introduction
Positive Life needs to keep certain information about its employees, volunteers and clients to allow it to monitor performance, achievements, and health and safety, for example.
It is also necessary to process information so that the organisation can comply with its legal obligations and staff can be recruited and paid, volunteers can be recruited, and service contracts met.
To comply with the law, information must be collected and used fairly, stored safely, and not disclosed to any other person unlawfully.
To do this, Positive Life must adhere to the Data Protection Principles, which are set out in the Data Protection Act 2018 (DPA 2018), and the General Data Protection Regulation (GDPR)

Policy Statement
The Board of Directors of Positive Life are committed to meeting their obligations under the Data Protection Act 2018. They will ensure that data collected and used will be relevant to its legitimate purposes and will not be prejudicial to the interests of board, volunteers or service users. Anyone involved in the processing of personal data will comply with the eight principles of good practice as follows;

- Fairly and lawfully processed
- Processed for legitimate purposes
- Adequate, relevant and not excessive
- Accurate
- Not kept longer than necessary
- Processed in accordance with the data subject's rights
- Secure
- Not transferred to other countries without adequate protection.

Policy Responsibility
The Chief Executive of Positive Life has the responsibility for ensuring that this policy is implemented effectively.
All staff or others who process or use personal information must ensure that they follow these principles at all times. All new staff will be made aware of this policy.

This policy should be read in conjunction with Positive Life's

- Data Sharing Checklist
- Confidentiality Policy
- Managing Subject Access Requests
- Privacy Notice.

The Data Controller and the Data Protection Officer
The organisation as a body corporate is the Data Controller under the 2018 Act, and the Board of Directors are therefore ultimately responsible for implementation. However, the Data Protection Officer (DPO) will deal with day-to-day matters.
The DPO for Positive Life is the Corporate Services Manager (CSM).
Any member of staff, volunteer or service user who considers that the Policy has not been followed in respect of personal data about him- or her-self should raise the matter with either the CEO or the CSM.

Role of the DPO
The Data Protection Officer role is assigned to a member of staff on a voluntary basis i.e. we are not legally obliged to have a DPO. We have chosen to do so as part of demonstrating our accountability and ensuring our compliance with data protection requirements.
The DPO assists Positive Life to:

- Monitor our internal compliance

- Inform and advise on our data protection obligations
- Act as a contact point for data subjects and the Information Commissioner's Office
- Advise the Board and staff on data protection matters.

The DPO is easily accessible as a point of contact for staff for data protection issues and is identified as the point of contact in our privacy notice and other external material. The DPO also will:

- Identify, organise, deliver training for staff, and meet with new staff during their induction to discuss data protection matters, including this policy
- have appropriate knowledge of data protection law and best practice, and are provided with adequate resources to help them carry out their role
- be nominally responsible for carrying out responses to requests made by data subjects, reporting breaches and drawing up policies and procedures.

This does not preclude another responsible member of staff for carrying out these duties.

Using Personal Data of Staff, Associates & Volunteers

We use your personal data to carry out recruitment, manage the employment relationship, and meet requirements set down by law.
When you apply for a position with Positive Life, we keep your application form for the duration of your employment and for a period up to two years after you leave.
The legal bases that we use for processing are

- Performance of a contract, to meet legal obligations, and where it is in our legitimate interest
- To process some sensitive personal data for equal opportunity monitoring purposes.

We keep your information secure and access to your personnel file is limited to HR and senior management.
We do not share your information with third parties other than as outlined in this notice, unless required to do so by law.
Your information is not stored outside of the European Union or transferred to international organisations.

You have the right to access your own information.
You do not have to provide what we ask for in most cases, but it may affect your application if you don't provide the information.

If you have a data protection question or request please contact the Data Protection Officer

Staff Obligations

All Staff are responsible for:

- Ensuring that any information they provide to the organisation in connection with their employment is accurate and up to date
- Informing the organisation of any changes to information that they have provided, e.g. changes of address, either at the time of appointment or subsequently

Positive Life cannot be held responsible for any errors unless the staff member has informed them of such changes.

When, as part of their responsibilities, staff collect information about other people (e.g. about an associate / volunteer or service users personal circumstances) they must comply with the guidelines as set out in the organisation's Data Retention Policy – see below.

Volunteer Obligations
All Volunteers are responsible for:

- Ensuring that any information that they provide to the organisation in connection with their volunteering is accurate and up to date
- Informing the organisation of any changes to information that they have provided, e.g. changes of address, either at the time of volunteering or subsequently.

Positive Life cannot be held responsible for any errors unless the volunteer has informed them of such changes.

If and when, as part of their responsibilities, an associate / volunteer collects information about other people (e.g. about a service users personal circumstances) they must comply with the guidelines as set out in the organisation's Data Retention and Confidentiality Policies.

Using Personal Data of Service Users
We use your personal data to

- Carry out support planning, assessment and reviews
- Ensure responsive service provision
- Inform funder monitoring requirements
- Meet relevant business needs.

We keep your information secure and access to your case file is limited to relevant support staff and senior management.
We do not share your personal information with third parties other than as agreed with you, unless required to do so by law.
Your information is not stored outside of the European Union or transferred to international organisations.

You have the right to access your own information.
You do not have to provide some of what we ask for, but it will affect the services that we are able to provide for you if you decide not to provide it

From time to time we may wish to use non-personal data for other purposes e.g. to assist with research. This will only be done with your specific opt-in permission.

If you have a data protection question or request please contact the Data Protection Officer

Service User Obligations
Service Users must ensure that all personal data provided to the organisation is accurate and up to date. They must ensure that changes of address etc. are notified to the relevant member of staff.

If, as part of their engagement with Positive Life and its services, service users have access to information about other people (e.g. another client's personal circumstances) they must comply with the guidelines as set out in the organisation's Data Protection and Confidentiality Policies.

DATA RETENTION POLICY & PROCEDURES

Data Security
All staff are responsible for ensuring that:

- Any personal data that they hold is kept securely. Filing cabinets / drawers must be kept locked and electronic information should be password protected
- The email checklist provided should be referred to in all instances prior to sending an email
- Group service user emails may only be sent by designated members of staff. The Corporate Services Manager will advise as appropriate
- All group external emails should be sent using 'BCC' unless there is a specific business reason to the contrary
- Beware of autocomplete on email. Check you are sending to the right address
- They adhere to the clear desk policy
- Personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

Staff must note that unauthorised disclosure will be a disciplinary matter, and may be considered gross misconduct.

Data Minimisation & Control
Data collection processes will be reviewed at least bi-annually by all staff to ensure that personal data collected and processed is kept to a minimum.
We will keep the personal data that we collect, use and share to the minimum amount required to be adequate for its purpose.
Where we do not have a legal obligation to retain some personal data, we will consider whether there is a business need to hold it.
We will retain personal data only for as long as it is necessary to meet its purpose. Our approach to retaining and erasing data no longer required is specified below. This schedule will be reviewed annually.
In the case of sharing personal data with any third party, only the data that is necessary to fulfil the purpose of sharing will be disclosed.
Anonymisation and pseudonymisation of personal data stored or transferred will be used where this is possible.

Rights to Access information
All staff, volunteers, and service users are entitled to:

- Know what information the organisation holds and processes about them and why
- Know how to gain access to it
- Know how to keep it up to date
- Know what the organisation is doing to comply with its obligations under the 2018 Act.

The organisation will, upon request, provide all staff, volunteers, and clients with a statement regarding the personal data held about them.
This will state all the types of data the organisation holds and processes about them, and the reasons for which they are processed.
All staff, volunteers and clients have a right under the 2018 Act to access certain personal data held about them either on computer or in certain files. Any person who wishes to exercise this right should submit a Subject Access Request to the CSM or CEO – see Managing Subject Access Request Policy.
The organisation aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 30 days, as required by the 2018 Act.

Data Retention

Service Users

- Positive Life's legal basis for holding service user information is consent.
- Service user information will be kept for two years. This time frame makes reasonable provision for service users who may periodically disengage with services but who might want to reengage as personal circumstances change. This reduces the need to repeat basic data gathering which might hinder reengagement.
- On request from a service user, data will be considered inactive and archived, electronically and / or in paper form as relevant.
- Data will be archived for two years and be considered inactive. It will be referred to only if it is required at request through formal channels for use in a legal case. After two years personal data will be destroyed.
- A service user may seek a variation to the above by making their request in writing to the Chief Executive.
- Each request will be dealt with on an individual basis and any decision based on the reasons for the request.

Volunteers and Associate Staff

- Access NI certificates will be retained for up to maximum of 1 month after which time a note of the date issued and certificate number will be kept on the individuals file.
- A Volunteer or Associate's information will be considered 'active' for one year from their last active engagement, except where there is an expressed arrangement e.g. a leave of absence. This will enable Positive Life to refer to documents should there be a reference request.
- The documentation will then be archived for two years and be considered inactive. It will be referred to only if it is required at request through formal channels for use in a legal case. After two years the data will be destroyed.
- A Volunteer or Associate may seek a variation to the above by making their request in writing to the Chief Executive.
- Each request will be dealt with on an individual basis and any decision based on the reasons for the request.

Employed Staff

- Access NI certificates will be retained for up to 1 month after which time a note of date issued and certificate number will be kept on the individuals file.
- Staff information will be considered 'active' for two years following the last date of employment. This will enable Positive Life to refer to documents should there be a reference request.
- The documentation will then be archived for five years and be considered inactive. It will be referred to only if it is required at request through formal channels for use in a legal case. After five years the data will be destroyed.

To ensure good practice, Positive Life will complete a data cleanse every three years.

Subject Consent

In many cases, the organisation can only process personal data with the consent of the individual. In some cases, if the data is sensitive, as defined in the 2018 Act, express consent must be obtained. Agreement to the organisation processing some specified classes of personal data is a condition of acceptance as a user of services, as a condition of volunteering by volunteers, and as a condition of employment for staff. This includes information about previous criminal convictions. Some roles will bring the applicants into contact with children.

The organisation has a duty under the Children (NI) Order 1995 and other enactments to ensure that staff are suitable for the post, and volunteers for their roles.
The organisation also has a duty of care to all staff, volunteers and service users and must therefore make sure that employees and those who use the organisation's premises do not pose a threat or danger to other users.

Processing Sensitive Information
Sometimes it is necessary to process information about a person's health, criminal convictions, race, and trade union membership.
This may be to ensure that the organisation is a safe place for everyone, or to operate other organisation policies such as the sick pay policy or the equal opportunities policy. Because this information is considered sensitive under the 2018 Act, staff (and volunteers and service users where appropriate) will be asked to give their express consent for the organisation to process this data.

The application forms that prospective staff, volunteers, and service users are required to complete will include a section requiring consent to process the applicant's personal data.
A refusal to sign such a form will prevent the application from being processed.
More information about this is available from the Chief Executive.

Reporting Breaches
A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
All members of staff should be vigilant and able to identify a suspected personal data breach. A breach could include:

- Loss or theft of devices or data, including information stored on USB drives or on paper
- Hacking or other forms of unauthorised access to a device, email account, or the network
- Disclosing personal data to the wrong person, through wrongly addressed emails, or bulk emails that inappropriately reveal all recipients email addresses
- Alteration or destruction of personal data without permission.

Where a member of staff discovers or suspects a personal data breach, this must be reported to the DPO immediately.
Where there is a likely risk to individuals' rights and freedoms, the DPO will report the personal data breach to the ICO within 24 hours of the organisation being aware of the breach.
Where there is also a likely high risk to individuals' rights and freedoms, Positive Life will inform those individuals without undue delay.
The DPO will keep a record of all personal data breaches reported, and follow up with appropriate measures and improvements to reduce the risk of reoccurrence.

Conclusion
Compliance with the 2018 Act is the responsibility of all directors, staff, associates, volunteers and service users of the organisation.
Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to organisation facilities being withdrawn, or even to a criminal prosecution.

Any questions about the interpretation or operation of this policy should be taken up with the Chief Executive.

Additional Reading:

- Managing Subject Access Request Policy
- Confidentiality Policy
- Privacy Notice