Data Protection Policy

This policy gives an overview of how we collect, process and use individual's personal data. More detail on some issues can be found in our Confidentiality Policy, Privacy Policy, Record of Processing Activities (ROPA), Data Protection Impact Assessment (DPIA) and Legitimate Interests Assessment (LIA).
This policy also acts as our Data Retention & Disposal Policy, Subject Access Requests Policy, Legitimate Interests Policy and Data Breach Reporting Policy

Organisation details

- Organisation Name: Interest Link Borders
- Organisation is a Data Controller.
- There is no Data Protection Officer. Data Protection Champion is Andrew Findlay Volunteer Hall, Langtongate, Duns TD11 3AF andrewfindlay@interestlink.org.uk 01573 410760 or 07785 734992

1. The 7 GDPR key principles in the context of Interest Link

1. Lawfulness, fairness & transparency. We have a valid reason (service provision) for collecting and using personal information. We use it fairly and we are clear, open and honest about how it will be used. See Lawful Basis and Individual Rights sections below.
2. Purpose limitation: We are clear about our purposes for collecting and using information. See Purposes section below.
3. Data Minimisation: The data we collect and process is adequate for the purpose, relevant to it and limited to what is necessary.
4. Accuracy: Our systems enable us to keep personal information updated and correct.
5. Storage limitation. See Retention Schedules below
6. Integrity and confidentiality (security). We keep most information in hard copy in locked filing cabinets in locked offices. Information kept electronically is kept to a minimum and has an appropriate level of security: it is in encrypted files on password-protected un-networked computers, and backups are to an encrypted cloud service.
7. Accountability. We have a Privacy Policy, Data Protection Policy and Confidentiality Policy. See section on Accountability & Governance below.

2. Personal data

Personal data is information identifying an individual directly or indirectly in combination with other information. Principal identifiers in our documentation are names, contact details and photos/video. We do not use identification numbers or location data or online identifiers.

3. Our purposes for processing information

- We collect and process information about members, carers and volunteers for the purpose of providing our befriending service.
- We process information about staff members to make recruitment decisions, administer payroll & pensions and provide supervision and support.
- We process information on directors for registration at Companies House and annual returns.
- We process information on directors and Branch Committee members to distribute papers and organise meetings.

A Data Protection Impact Assessment has been carried out because the service uses health data to decide on access to the service (learning disabilities must be present).

4. Lawful basis for processing information

Consent

Although we rarely rely on it as the sole lawful basis of processing data under GDPR, we obtain written consent from members, carers and volunteers on Request for Service forms, Volunteer Application forms and additional specific consent forms. Requests are prominent, separate from other information and require a positive opt-in; records of consents are kept and consents are refreshed if anything changes.

- We ask for consent to use photos and video in publicity and reporting.
- Some member information comes from other sources such as teachers, health & care professionals. We ask for consent on Request for Service forms to collect this information and also to share information with volunteers.
- Some of our members have a lack of capacity to provide consent. Carers' consent on Request for Service forms addresses this to a large degree, but it is a reason to have an additional lawful basis beyond consent.
- Parents of volunteers under 13 are asked for their consent to us requesting information from a referee.

Legitimate Interests

- For members, carers, volunteers, staff and committee members an additional legal basis for is legitimate interests: we need to collect and process the information to provide and evaluate the service and manage the organisation.
- The Information Commissioners Office has confirmed that these legitimate interests are a sound basis on which a befriending service can process information.

Special Category Data and Criminal Convictions and Offence Data

- Special Category Data: Health. This principally relates to members (although some health information may involve volunteers or staff. We rely on GDPR Article 9(2)(a) consent and Article 9(2)(h) social care
- Criminal Convictions and Offence Data: we process this in connection with volunteer, staff and director PVG Scheme Applications. We rely on Data Protection Act 2018 Sch.1, Pt.1, 2 - social care & Sch.1, Pt.2, 29 consent
- The Information Commissioners Office has confirmed that befriending services are social care services for GDPR and DPA purposes.

Other:

- Contract and legal obligation are additional lawful bases for processing staff information.
- Legal obligations re Companies House and Annual Accounts cover elements of data processing re directors.

5. Individual Rights.

Right to be informed

At the time of collecting personal data, we provide individuals with concise, transparent intelligible and easily accessible privacy information written in clear and plain language. This includes:

- Our purposes for processing their personal data,
- Our retention periods for that personal data, and
- Who it will be shared with.

Rights of access to, rectification of and erasure of data: we give information about these rights on Request for Service and Volunteer Application forms.

Rights to restrict processing, to have data portability, and to make objection to the use of data have special features and are unlikely to be invoked in relation to our service.

6. Subject Access requests: also see Privacy Policy

Any individual has the right to see what personal information we hold about them. They are entitled to be given confirmation as to whether we hold or process their personal information, and if so they are entitled to access all their personal information as well as details of:

- The purposes for which we process their personal data;
- The categories of their personal data we process;
- The recipients, or categories or recipient to whom personal data has been or will be disclosed
- How long we expect to store their data;
- Where they did not give us the personal data, the source from which we collected the personal data.

They are entitled to have any mistakes in their personal data rectified, and to have the data deleted if they would no longer like us to store or process their personal data, or to request restriction of our processing of their personal data.

7. Accountability & Governance

A Record of Processing Activities (ROPA) is maintained which satisfies GDPR Article 30 and Data Protection Act 2018 requirements re Special Category or Criminal Conviction and Offence data

8. Annual Data Protection Fee

There is an exemption for not-for-profit organisations, and we satisfy the requirements of it.

9. No Data Protection Officer (DPO) registered with ICO.

We are not processing special categories of data on a large scale so do not need a DPO. To avoid confusion the Interest Link staff member responsible for information security and management is called the Data Protection Champion. This is currently the Project Co-ordinator.

10. Data Retention & Disposal Policy

- Member, Volunteer and Staff files (including computer files) are kept for 6 years after they leave the service or organisation. Pension records are kept for 75 years post-employment.
- Information on our database/register of Members and Volunteers is also kept for 6 years after leaving the service or organisation.
- PVG Scheme Records and Record Updates are shredded as soon as a recruitment decision has been made.
- Records of group activities (including group risk assessments) are kept for 6 years from date of activity.
- Accounting records (which contain information on committee members, staff and volunteers through their expenses claims) are kept for 6 years from financial year-end.
- Hard-copy marketing materials that include photographs of individuals, such as posters, leaflets and pull-up banners are replaced every 6 years at maximum.
- Website and Social media content: photographs of individuals are replaced every 6 years at maximum.
- Evaluation material containing photos (e.g. photoreports, independent evaluations, Impact Reports and Films) is kept indefinitely in hard copy and digital archive and are accessible for up to 6 years through our website. Survey questionnaires are shredded once the information has been transcribed into electronic file.
- Destruction of Branch files is the responsibility of the relevant Branch Co-ordinator. Otherwise the Project Co-ordinator has responsibility for ensuring data is disposed of on schedule.

11. Data breaches: also see Data Protection Impact Assessment (DPIA)

- A breach occurs if there is an accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- Likely breaches might be through an email being sent to the wrong person, someone outside the organisation gaining access to a filing cabinet, or the loss or theft of a laptop or paper files
- If there is a confirmed or suspected breach of personal data, the staff member discovering it should contact the Project Co-ordinator immediately.
- The Project Co-ordinator and staff involved will try to contain the breach, minimise its effects and recover any data where possible.
- They will investigate the breach and assess the risks associated with it (for example, identity theft, fraud, safety of members, reputational damage) the potential adverse consequences for individuals, how serious or substantial those are and how likely they

are to occur. If it is likely there will be a risk to people's rights and freedoms then the data subject(s) and the Information Commissioners Office will be notified immediately.

- A record of the breach, together with any action taken to remedy it and prevent its recurrence will be made on an Incident Report form. A report will also be made by the Project Co-ordinator to the Interest Link Board, either immediately or in the next bi-monthly report depending on the seriousness of the breach.
- If the breach is the result of an inappropriate disclosure by a volunteer or staff member it may also be a disciplinary matter and be dealt with in accordance with our disciplinary procedures.