Bolton Dementia Support
Living well with dementia.

Data Protection Policy

Last updated	October 2018

Definitions

Organisation	Means Bolton Dementia Support
GDPR	Means EU General Data Protection Regulation
Responsible Person	Means Alison Lowe Chief Officer
Register of Systems	means a register of all systems or contexts in which personal data is processed by the organisation e.g. IT – use of passwords and any encrypted files, how files are stored, shredding of confidential data, use of shared drive and cloud systems, use of security systems and firewalls.

1. Bolton Dementia Support needs to gather and use certain information about individuals. These can include volunteers, staff, users of our service and other people the organisation has a contact with and may need to contact. For e.g. our membership database records. Risk Assessments. Publicity relating to fundraising and donations, emergency contacts when organising activities, case work. Staff supervision notes and recruitment. This policy describes how this personal data must be collected, handled and stored to meet the organisation's data protection standards and to comply with the law. We intend to comply with our legal obligations under the Data Protection Act 2018 (the '2018 Act') and the EU General Data Protection Regulation ('GDPR') in respect of data privacy and security. We have a duty to notify you of the information contained in this policy.

This Policy ensures **Bolton Dementia Support**

- Complies with data protection law and follows good practice
- Protects the rights of volunteers, staff and anyone that uses the service

- Is open about how its stores and processes individuals' data
- Protects itself from the risk of data breach

2. General Provisions

The Responsible Person shall take responsibility for the Organisation's ongoing compliance with this policy.

This policy shall be reviewed at least annually.

The Organisation shall register with the Information Commissioner's Office as an organisation that processes personal data **unless exempt.**

3. Data protection principles

Bolton Dementia Support is committed to processing data in accordance with its responsibilities under the GDPR.

This requires that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

To this end Bolton Dementia Support will take responsibility for complying with the GDPR. at the highest management level and throughout the organisation. We put in place appropriate technical and organisational measures and we review and update our

accountability measures at appropriate levels.

4. How we define personal data

Personal data' means information which relates to a living person who can be identified from that data (a 'data subject') on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.

For e.g. personal data provided by users of the service, or someone else (such as a former employer, or it could be created by the group. It could be provided or created during recruitment processes (of volunteers and/or staff) or during the course of a contract of employment (or services) or after its termination. It could be created by a line manager or other colleagues. Examples may include:
Membership details, application forms and CV's, references, contact details and date of birth; the contact details for your emergency contacts; gender; marital status and family details; contract of employment (or services), working hours, salary, pension, benefits and holiday entitlement; bank details, tax status, national insurance number; passport and driving licence, immigration status and right to work; disciplinary or grievance investigations and proceedings; performance and behaviour at work; electronic information in relation to your use of IT systems/swipe cards/telephone systems and calendars; images by photographs.

5. Lawful, fair and transparent processing

To ensure its processing of data is lawful, fair and transparent, the Organisation shall maintain a Register of Systems.

The Register of Systems shall be reviewed at least annually.

All individuals who are the subject of personal data held by Bolton Dementia Support are entitled to:

- Ask what information the Organisation holds about them and why
- Ask how to gain access to it
- Be informed how to keep it up to date
- Be informed how the Organisation is meeting its' data protection obligations.

If an individual contact the Organisation requesting this information, this is called a subject access request. This should be made in writing and passed to the Responsible Person. Any requests made to the Organisation shall be dealt with in a timely manner.

6. Lawful purposes

- All data processed by the Organisation must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests (see ICO guidance for more information).

So to check a person has the legal right to work for the organisation; to carry out a contract; training you and reviewing your performance; to decide whether to promote you; to determine whether to make reasonable adjustments in the workplace or role because of disability; to monitor diversity and equal opportunities, to monitor and protect the security of the Organisation; volunteers staff and others; to monitor and protect health and safety of volunteers, staff and others; to pay salaries and expenses; to provide references; to comply with our legal obligations; the prevention and detection of fraud or other criminal offences.

- The Organisation shall note the appropriate lawful basis in the Register of Systems.
- Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
- Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Organisation's systems.

7. Data minimisation

- The Organisation shall ensure that personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Data is held in as few places as necessary, taking every opportunity to ensure data is kept up to date, and data will only be kept if necessary, deleting data we don't need.

8. Accuracy

- The Organisation shall take reasonable steps to ensure personal data is accurate.
- Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

  This will be reviewed regularly.

9. Archiving / removal

- To ensure that personal data is kept for no longer than necessary, the Organisation shall put in place an archiving policy for each area in which personal data is processed and review this process annually.
- The archiving policy shall consider what data should/must be retained, for how long, and why.

10. Security

- The Organisation shall ensure that personal data is stored securely using modern software that is kept-up-to-date.
- Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
- When personal data is deleted this should be done safely such that the data is irrecoverable.
- Appropriate back-up and disaster recovery solutions shall be in place.

Ensure everyone is locking computer screens when away from desks, not sharing data informally or via unsecure communication systems and networks, not saving copies of personal data to personal computers. Passwords are changed frequently. Data is backed up on a secure server. Offices are always locked, and cabinets are locked if they contain personal data.

11. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Organisation shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO. (more information on the ICO website).

Date of Review: October 2019

Ratified by Trustees 18.7.2019