


BGNS	Data Protection Policy and Procedures	
------	---------------------------------------	---

Please note: the terms Steering group and Committee are coterminous.

We are committed to a policy of protecting the rights and privacy of individuals. We need to collect and use certain types of data in order to carry on our work of providing services to our care scheme users and supporting the recruitment and administration of our volunteers. This personal information must be collected and handled securely.

The Data Protection Act 2018 (DPA) and General Data Protection Regulations (GDPR) govern the use of information about people (personal data). Personal data can be held on computers, laptops and mobile devices, or in a manual file, and includes email, minutes of meetings, and photographs.

The good neighbours / care scheme will remain the data controller for the information held. The steering group and volunteers are personally responsible for processing and using personal information in accordance with the Data Protection Act and GDPR. Steering group members and volunteers who have access to personal information will therefore be expected to read and comply with this policy.

Purpose

The purpose of this policy is to set out the [scheme name] commitment and procedures for protecting personal data. Steering group members regard 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 with. We recognise the risks to individuals of identity theft and financial loss if personal data is lost or stolen.

Principles of GDPR / the Data Protection Act

This contains 6 principles for processing personal data with which we must comply.

1. Lawfulness, fairness and transparency

- You must identify valid grounds under the GDPR (known as a 'lawful basis') for collecting and using personal data.
- You must ensure that you do not do anything with the data in breach of any other laws.
- You must use personal data in a way that is fair. This means you must not process the data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned.
- You must be clear, open and honest with people from the start about how you will use their personal data.

2. Purpose limitation

Organisations should only collect personal data for a specific purpose, clearly state what that purpose is, and only collect data for as long as necessary to complete that purpose.

- You must be clear about what your purposes for processing are from the start.
- Bedfordshire Care Scheme Data Protection Policy Template - GDPR Page 2 of 2
- You need to record your purposes as part of your documentation obligations and specify them in your privacy information for individuals.
- You can only use the personal data for a new purpose if this is compatible with your original purpose, you get consent, or you have a clear basis in law.

3. Data minimisation

You must ensure the personal data you are processing is:

- adequate – sufficient to properly fulfil your stated purpose;
- relevant – has a rational link to that purpose; and

- limited to what is necessary – you do not hold more than you need for that purpose.

4. Accuracy

The accuracy of personal data is integral to data protection. The GDPR states that “every reasonable step must be taken” to erase or rectify data that is inaccurate or incomplete.

Individuals have the right to request that inaccurate or incomplete data be erased or rectified within 30 days.

- You should take all reasonable steps to ensure the personal data you hold is not incorrect or misleading as to any matter of fact.
- You may need to keep the personal data updated, although this will depend on what you are using it for.
- If you discover that personal data is incorrect or misleading, you must take reasonable steps to correct or erase it as soon as possible.
- You must carefully consider any challenges to the accuracy of personal data.

5. Storage limitation

Similarly, care schemes need to delete personal data when it is no longer necessary.

- You must not keep personal data for longer than you need it. Client data can be destroyed once they no longer require the scheme services. Volunteer data should be kept for as long as the volunteer is active in the scheme.
- You need to think about – and be able to justify – how long you keep personal data. This will depend on your purposes for holding the data.
- You need a policy setting standard retention periods wherever possible, to comply with documentation requirements.
- You should also periodically review the data you hold, and erase or anonymise it when you no longer need it.
- You must carefully consider any challenges to your retention of data. Individuals have a right to erasure if you no longer need the data.

- You can keep personal data for longer if you are only keeping it for public interest archiving, scientific or historical research, or statistical purposes.

6. Integrity and confidentiality

This is the only principle that deals explicitly with security. The GDPR states that personal data must be “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”.