Bridgend Centre

Privacy/GDPR policy

The Bridgend Centre (Bollington Community Association) is committed to protecting and respecting people's privacy.

This policy explains when and why we collect personal information about people, how we use it, the conditions under which we may disclose it to others and how we keep it secure.

We may change this policy from time to time, so individuals should request the most up to date version of the policy when obtaining information on it. Any questions regarding it should be directed to Centre Manager, Bridgend Centre, 104 Palmerston Street, Bollington, Cheshire, SK10 5PW.

There are a number of Appendices to accompany this policy and these are listed in full in section 13.

1. Statement of policy

The Bridgend Centre ("organisation") needs to keep certain information on its employees, volunteers, service users and trustees to carry out its day-to-day operations, in order to respect people's privacy and to comply with legal obligations.

The organisation is committed to ensuring any personal data will be dealt with in line with the Data Protection Act and the General Data Protection Regulation policy (GDPR). To comply with the law, personal information will be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

Personal data can be held on computers, laptops and mobile devices, or in a paper file and includes email, minutes of meetings and photographs.

The aim and purpose of this policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures. This document also highlights key data protection procedures within the organisation.

Under the GDPR act, the Bridgend Centre is the *data controller* and also a *data processor* for the information being held. The trustees, staff and volunteers are personally responsible for processing and using personal information in accordance with GDPR and will therefore be expected to read and comply with this policy.

2. Principles of the GPDR

Article 5 of the GDPR requires that personal data:

a) Shall be processed fairly and lawfully and in particularly shall not be processed unless specific conditions are met,

b) Shall be obtained only for one or more of the purposes specified in the act and shall not be processed in any manner incompatible with that purpose or purposes,

c) Shall be adequate, relevant and not excessive in relation to those purpose(s),

d) Shall be accurate and kept up to date

e) Shall not be kept for longer than is necessary

f) Shall be processed in accordance with the rights of the data subjects under the Act,

g) Shall be 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

h) Shall not be transferred to a country or territory outside the European Economic Area unless that country ensures an adequate level of protection for the rights and freedoms of data subjects.

The GDPR applies to both data 'controllers' **and** 'processors'.

- A **controller** determines the purposes and means of processing personal data.
- A **processor** is responsible for processing personal data on behalf of a controller.

The Bridgend Centre is both a controller and a processor with regards to the various personal data and processing activities carried out by the organisation. Therefore, it is important that the Bridgend Centre complies with the principles above at all times in relation to these activities and also ensures any third-party contractors who carry out these processes on the organisation's behalf do so too.

3. Definitions

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified; in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

4. Lawful bases for processing

There are six lawful bases for processing data under GDPR (under Article 6), and the organisation must ensure that each process falls under these and has been documented, together with the reasoning behind this.

These bases are:

a) **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.
b) **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
c) **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
d) **Vital interests:** the processing is necessary to protect someone's life.
e) **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
f) **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

The Bridgend Centre has documented each process in which it processes personal data and has detailed the bases for doing this, together with the rationale behind this decision. This is available in detail in the audit in Appendix 1.

Special category data

The categories of data marked with an * in the data audit are classed as 'special category data' under GDPR. We will minimise the collection of special category data and only do so when legally or contractually required or if there is a specific purpose.

Children

The Bridgend Centre may only hold a small amount of personal data that relates to an individual who is a child. If we do collect personal data about a child the organisation will always use the lawful basis of consent and ensure that its information is written in a way that children will understand their rights.

Children aged 13 and over are able to provide their own consent and for children under this age written consent will be gathered from whoever holds parental responsibility for that child.

5. Individual rights under GDPR

The GDPR provides the following rights for individuals:

5.1 The right to be informed

The Bridgend Centre has an obligation to inform every individual about what information the organisation processes about an individual. This information is provided through 'privacy notices' to the individual.

5.2 The right of access

Individuals have a right to access their personal data held by the organisation. They also have the right to be aware of what legal bases the organisation is holding and/or processing their data under GDPR.

The process for the individual to follow to request access to their data is called a 'Subject Access Request' and is detailed in Appendix 2.

5.3 The right to rectification

The GDPR gives individuals the right to have personal data rectified. Personal data can be rectified if it is inaccurate or incomplete.

The process for the individual to follow to request that their data be rectified can be found in Appendix 2.

If we are not able to comply with any request you make to rectify your data, we will inform you within one month of receipt of the request with clear reasons. You would then have the right to make a complaint regarding this decision to the Information Commissioner's Office.

5.4 The right to erasure

Under GDPR, individuals have the 'right to be forgotten', i.e. they have the right to have their data erased where there is no compelling reason for its continuing to be processed.

There are circumstances where the individual can request that their data be erased, which can be found in Appendix 2. However, there are also some circumstances where the organisation has a right to refuse this request. For example, in situations where there is a legal obligation to keep it, such as for Gift Aid donations or payroll data.

If we are not able to comply with any request you make to erase your data, we will inform you within one month of receipt of the request with clear reasons. You would then have the right to make a complaint regarding this decision to the Information Commissioner's Office.

5.5 The right to restrict processing

Individuals have a right to 'block' or suppress processing of personal data. When processing is restricted, the organisation is permitted to store the personal data, but not further process it.

Examples of the situations when this would apply are likely to be where an individual contests the accuracy of the personal data and so the organisation should restrict the processing until they have verified the accuracy of the personal data or when processing is unlawful and the individual opposes erasure and requests restriction instead

The organisation can retain just enough information about the individual to ensure that the restriction is respected in future.

If we are not able to comply with any request you make to do this, we will inform you within one month of receipt of the request with clear reasons. You would then have the right to make a complaint regarding this decision to the Information Commissioner's Office.

5.6 The right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.

This means that if an individual requests their data, the organisation must supply the information in an easy to access and read digital format within one month of the request. There must be no charge for providing this information.

If the individual requests it, the organisation must transfer the data to another organisation, where technically possible.

If we are not able to comply with any request you make to do this, we will inform you within one month of receipt of the request with clear reasons. You would then have the right to make a complaint regarding this decision to the Information Commissioner's Office.

5.7 The right to object

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

Individuals must have an objection on "grounds relating to his or her particular situation".

The organisation must stop processing the personal data unless:

- you can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- the processing is for the establishment, exercise or defence of legal claims.

The organisation must inform individuals of their right to object "at the point of first communication" and in our privacy notice.

This must be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information".

If we are not able to comply with any request you make to rectify your data, we will inform you within one month of receipt of the request with clear reasons. You would then have the right to make a complaint regarding this decision to the Information Commissioner's Office.

5.8 Rights in relation to automated decision making and profiling.

The GDPR has provisions on:

- automated individual decision-making (making a decision solely by automated means without any human involvement); and
- profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

The Bridgend Centre does not carry out any automated decision-making or profiling on its data.

6. Accountability and governance

The GDPR promotes accountability and governance for organisations who handle personal data and they are expected to put comprehensive but proportionate governance measures in place.

This includes:

- relevant audits and documentation on data processing activities
- implement appropriate technical and organisational measures that ensure and demonstrate that the organisation complies.
- implement measures that meet the principles of data protection. Measures could include:
    - data minimisation;
    - pseudonymisation;
    - transparency;
    - allowing individuals to monitor processing; and
    - creating and improving security features on an ongoing basis.
- use data protection impact assessments where appropriate.

6.1 Contracts

When a data controller uses a processor, a written contract must be in place around GDPR. The contract lays out what the responsibilities and liabilities are for both parties.

This has implications for the Bridgend Centre which acts as both a data processor (for example to a funder who requests statistical information) and as a data controller which uses a processor (for example Bridgend's payroll provider is a processor on the organisation's behalf). If we are required to share statistical or personal information with a funder, we will inform you.

The detail that must go in the contract is detailed in the GDPR legislation and the Bridgend Centre will ensure that it complies.

An example contract can be found in Appendix 4.

6.2 Documentation

The GDPR contains explicit provisions about an organisation documenting their processing activities. The organisation must maintain records on several things such as processing purposes, data sharing and retention.

The Bridgend Centre's data processes are recorded in Appendix 1.

7. Data security

The GDPR requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. It requires that appropriate technical or organisational measures are used.

The Bridgend Centre will ensure that all required necessary security processes and interventions are in place. This will include relevant information technology and communication security, data processes and staff training.

General data security procedures can be found in Appendix 6 and specific home-working security procedures can be found in Appendix 5.

8. Personal data breaches

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. Organisations must do this within 72 hours of becoming aware of the breach, where feasible.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the individual must also be informed without undue delay.

Organisations should ensure they have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority and the affected individuals.

Organisations must also keep a record of any personal data breaches, regardless of whether or not they are required to be notified.

The Bridgend Centre policy and procedure on this can be found in Appendix 3.

9. Privacy Notice

Being transparent and providing accessible information to individuals about how we will use their personal data is a key element of the Data Protection Act 1998 (DPA) and the EU General Data Protection Regulation (GDPR). The most common way to provide this information is in a privacy notice.

The Bridgend Centre's privacy notice can be found in Appendix 7 and is also published on our website. A paper copy can be obtained by contacting the Centre Manager, who can also provide further detail on information processed and held by the organisation.

10. Responsibilities

Under the Data Protection Guardianship Code, overall responsibility for personal data in a not for profit organisation rests with the governing body. In the case of Bridgend Centre this is the Board of Trustees.

All staff, trustees and volunteers who process personal information must ensure they not only understand but also act in line with this policy and the data protection principles.

Breach of this policy by employees will result in disciplinary proceedings and by trustees or volunteers will result in a review of their position within the organisation.

11. Training

Training and ensuring knowledge about the Data Protection Act and how it is followed in this organisation will take the following forms:

At their induction, staff, trustees and volunteers will be shown the processes required to follow in order to comply with the data protection act. They will also be required to read this policy and confirm that they have done so as well as understanding its contents.

General awareness training sessions to employees will be carried out on an annual basis.

12. Policy Review

This policy will be reviewed on an annual basis in order to ensure we keep up to date with GDPR law. This is unless we identify a need to review the policy earlier.

13. List of Appendices

Appendix 1 – Summary of data held by the Bridgend Centre

Appendix 2 – Subject access requests, requests for erasure, rectification, erasure, the right to object, the right to restrict processing and data portability

Appendix 3 – Data breach procedure

Appendix 4 – External supplier contract and checklist

Appendix 5 – Home working checklist – staff and trustees

Appendix 6 – Data protection day to day procedures

Appendix 7 – Bridgend Privacy Notice

This procedure has been approved & authorised by:

Name:

Position:

Date:

Signature: