



A really useful place for community groups

Prior House, 6 Tilbury Place, Brighton, BN2 0GY | 01273 606160
info@resourcecentre.org.uk | www.resourcecentre.org.uk
[fb.com/resourcecentrebh](https://www.facebook.com/resourcecentrebh) | [@ResourceCtrBH](https://twitter.com/ResourceCtrBH)

Data protection policy

This policy and the way in which it operates will be reviewed every 2 years by the staff team and the management committee. This policy was updated in December 2021.

Signed:

Date:

Director of B&H SWET Ltd (the employer)

Introduction and overview

1. General statement of policy

- 1.1. The policy of the Resource Centre is to respect and protect personal data of our users, staff and trustees, in line with the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018.
- 1.2. We collect, store, use, amend, share, destroy or delete personal data only in ways which respect people's privacy and comply with the relevant legislation.
- 1.3. We take a "by design and by default" approach to data protection, which means we take it into consideration when making arrangements for all aspects of running the Resource Centre.

2. Definitions

- 2.1. "We" is the Resource Centre, also known as Brighton and Hove Social Welfare and Educational Trust Ltd.
- 2.2. Personal data is information about a person which is identifiable as being about them. It can be stored electronically or on paper, and includes images and audio recordings as well as written information.
- 2.3. Data protection is about how we, as an organisation, ensure we protect the rights and privacy of individuals, and comply with the law, when collecting, storing, using, amending, sharing, destroying or deleting personal data.
- 2.4. The Resource Centre is the "Data Controller" for all data that we process. This means we collect and process data ourselves, to meet our own organisational purposes. We do not process data on behalf of third party organisations.
- 2.5. A "Data Subject" is a living person whose data is processed by or on behalf of the Resource Centre.
- 2.6. A "Data Processor" is an organisation who processes data on behalf of the Resource Centre.
- 2.7. "Special category data" is data that includes information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, health information, data concerning someone's sex life or sexual orientation, and biometric data that uniquely identifies someone.

Data processing

3. Purposes for processing

- 3.1. We will only process data when we have a clear purpose for doing so.
- 3.2. We will only process the minimum amount of data that is necessary to achieve the specific, identified purpose.
- 3.3. Data will not be kept longer than needed to achieve its purpose.
- 3.4. Data subjects will be informed of the purpose of the processing.
- 3.5. Data subjects may request access to their data, and we will provide them with a copy of their data in a format they can understand, within one month of a request.

- 3.6. We may maintain an archive of documents and photographs relating to the history of the Resource Centre, provided that:
- 3.6.1. We only keep the minimum amount of personal data necessary to maintain an archive in the public interest
 - 3.6.2. We do not keep personal data if this is likely to cause substantial damage or substantial distress to an individual
- 3.7. All purposes must be clearly and specifically identified as falling within one of the legal bases for processing data. These are:
- 3.7.1. purposes that are in the Resource Centre's legitimate interests, or
 - 3.7.2. purposes for which the data subject has given explicit consent, or
 - 3.7.3. contracts with the data subject, or
 - 3.7.4. to comply with legal obligations, or
 - 3.7.5. to protect someone's vital interests, or
 - 3.7.6. to perform public tasks.
- 3.8. Purposes for processing special category data must meet one of the legal bases listed in 3.7.1–3.7.6 *and* one of the following additional bases for processing special category data:
- 3.8.1. purposes for which the data subject has given explicit consent (including specific consent to process the special category data), or
 - 3.8.2. purposes of identifying or keeping under review the existence or absence of equality of opportunity or treatment between groups of people specified in relation to that category with a view to enabling such equality to be promoted or maintained. In order to generate aggregated statistics on the use of our services by different types of group (eg those whose members are BME, disabled, of a particular ethnic origin, faith or sexual orientation), we identify these types of group in our database. For some groups, we also record names and contact details of individual members of these groups who have requested support or who have given explicit consent for us to record their data. We do not use this special category data in order to make any decisions with respect to particular individuals and do not share this personal data beyond the Resource Centre.

4. Legitimate interests

- 4.1. We will process data in ways that meet the Resource Centre's legitimate interests.
- 4.2. A clear, legitimate interest must be identified, and the processing must be necessary in order to meet the legitimate interest.
- 4.3. This processing will only be done in ways that the data subject would reasonably expect.
- 4.4. Data subjects will be provided with information about the purpose of the processing, and how to have their details erased from our records.

5. Contracts

- 5.1. We will process data in ways that are necessary for us to fulfil contractual obligations with data subjects or to provide data subjects with information they have requested prior to entering into a contract (e.g. provide information about equipment availability, on request).

- 5.2. Data subjects will be provided with information about how to have their details erased from our records.
- 5.3. Data will not be kept for longer than needed to complete the contract and ensure any necessary follow-up work is possible.

6. Legal obligations

- 6.1. We will process data in ways that are necessary for us to meet our legal obligations.
- 6.2. Data will not be kept for longer than needed to allow us to meet our legal obligations.

7. Vital interests

- 7.1. If necessary, we will process data in ways that protect the life of a data subject or someone else's life.

8. Public tasks

- 8.1. As a voluntary organisation we do not perform public tasks, so will not use this legal basis for processing data.

9. Explicit consent

- 9.1. We will process data in ways for which we have explicit consent from the data subject.
- 9.2. Consent must be specific (data subjects should be able to consent to use of data for one purpose but not another).
- 9.3. Consent must be opt-in. Data subjects must actively give consent: consent cannot be assumed.
- 9.4. Where data is processed on the basis of consent, we will make it as easy to withdraw consent as it is to give it.
- 9.5. Data subjects will be provided with information about how to have their details erased from our records.

10. Data storage

- 10.1. Data will be stored securely in the Resource Centre server, which is located in the Resource Centre offices and is password protected.
- 10.2. Data will be backed up onto an encrypted external hard drive which will be stored in a staff member's home.
- 10.3. Data will be stored on a tablet which is password protected.
- 10.4. Data will be stored on staff computers in their homes which are password protected.
- 10.5. Data will also be stored in well-organised folders, filing cabinets and boxes in the Resource Centre. The vast majority of this will be stored away from the public areas of the Centre. Folders containing contact details for people to whom we are providing current services may be stored in the reception desk drawers. The reception is staffed at all times, and this data will not be stored there for longer than it is needed to provide the service.

11. Data erasure

- 11.1. Data deleted from the server is permanently deleted.
- 11.2. Deleted folders in email inboxes will be emptied automatically.
- 11.3. Personal data on paper will be shredded securely.

12. Use of data processors

- 12.1. We use a number of online platforms who process data on our behalf. We will only use data processors who confirm that they are UK GDPR compliant.
- 12.2. In particular, we will check that data is stored securely, that it can be accessed in a format that is easy to understand, that it can be permanently deleted on request, and that data is not transferred outside of the UK unless the transfer is compliant with Chapter V of the UK GDPR.

Accountability and governance

13. Responsibility

- 13.1. The Resource Centre Management Committee delegates overall responsibility for data protection to the workers' group.
- 13.2. The workers' group should ensure that the Management Committee receives necessary reports on data protection issues, and may call a special meeting of the Management Committee where a data protection related matter requires the Committee's urgent attention.
- 13.3. The workers' group is responsible for implementing arrangements for data protection throughout the organisation.

14. Documentation

- 14.1. We will maintain a record of purpose and legal basis for all non-occasional data processing, and any processing which includes special category data.
- 14.2. We will maintain a record of any non-occasional sharing of data.
- 14.3. We will maintain a record of any non-occasional retention of data, or retention of special category data.
- 14.4. We will maintain a record of data breaches, and actions that have been taken to mitigate their impacts and avoid them happening again in future.

15. Procedures

- 15.1. We will have a set of data protection procedures which outline purposes, legal bases, and specific guidance for workers about all regular data processing activities.
- 15.2. These procedures will be designed by the workers group and agreed by the management committee. They will be reviewed every 2 years, along with this policy.

16. Data breaches

- 16.1. Data breaches will be taken seriously and responded to in a timely manner.
- 16.2. The first step in response to any data breach is to try to minimise the impact of the breach. In the case of data that has been lost, stolen, or shared in error, we will make every effort to recover the data.
- 16.3. We will evaluate our procedures in response to data breaches, and take steps to ensure any mistakes are corrected for the future.
- 16.4. We will investigate every data breach to assess whether it may have an impact on the rights or freedoms of a data subject. Where this may be the case, data breaches will be reported to the data subject and to the ICO within 72 hours.