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 | @ResourceCtrBH

Data Protection Procedures

General

These procedures should be followed by staff at all times in order to ensure compliance with the UK General Data Protection Regulation and the Data Protection Act 2018, and maintain the privacy of staff, trustees and users of the Centre.

The procedures are based on the principles outlined in the Resource Centre's Data Protection Policy.

These procedures will be reviewed every two years by the staff team and ratified by the management committee.

These procedures were reviewed in March 2024.

Signed:

Date:

Director of B&H SWET Ltd (the employer)

Storing personal data

1. Provisional contacts

1.1. Provisional contact details are stored in the database when we:

1.1.1. Create an equipment booking. This data is stored on the basis of legitimate interest.

1.1.2. Create an unpaid invoice. This data is stored on the basis of contract.

1.2. Ensure that groups understand that we will only process their data in relation to the specific booking or invoice. Refer to the privacy notice for equipment bookings, on the Resource Centre website.

1.3. Provisional contact data that has been stored for more than four years will be deleted from the database annually (see part 8).

2. Group contacts

2.1. Group contact details are stored in the database when:

2.1.1. We undertake ongoing support work with a priority group

2.1.2. We agree to invoice a group monthly

2.1.3. We accept a booking for a regular print service job

2.1.4. A group's application for membership is approved by the Management Committee

2.1.5. We are given contact details for a tenant or resident association by Brighton & Hove City Council (BHCC) Housing Services

2.1.6. We are asked by an individual to add their details to the database for future reference

2.1.7. We send a reminder letter to an individual who is responsible for an unpaid invoice

2.2. For group contacts created under points 2.1.1 to 2.1.3 (priority groups and regular users):

2.2.1. This data is stored on the basis of legitimate interest. Tick the 'legitimate interest' box in the database when storing the data.

2.2.2. Check regularly when working with groups that these contact details are up to date and amend them as required

2.2.3. Group contact data for groups that have not used the Centre for more than four years will be deleted from the database annually (see part 8)

2.2.4. Refer to the privacy notice for member groups and regular users on the Resource Centre website

2.3. For group contacts created under point 2.1.4 (member groups):

2.3.1. This data is stored on the basis of legitimate interest. Tick the 'legitimate interest' box in the database when storing the data.

2.3.2. Check regularly when working with groups that these contact details are up to date and amend them as required.

2.3.3. Ensure that the Resource Centre Members list on Mailchimp is updated to match the database before using it to send out a mailing. Follow the Mailchimp updating procedure correctly to ensure that people who have unsubscribed from Mailchimp are not sent emails.

2.3.4. Group contact data for groups that have not used the Centre for more than four years will be deleted from the database annually (see part 8)

2.3.5. Refer to the privacy notice for member groups and regular users on the Resource Centre website

2.4. For group contacts created under point 2.1.5 (BHCC Tenants' and Residents' Associations):

2.4.1. This data is stored on the basis of legitimate interest. Tick the 'legitimate interest' box in the database when storing the data.

2.4.2. Update the database promptly in response to updated information from Housing Services

2.4.3. Refer to the privacy notice for member groups and regular users on the Resource Centre website

2.5. For group contacts created under point 2.1.6 (individuals who ask us to store their details):

2.5.1. This data is stored on the basis of explicit consent. Tick the 'consent' box in the database when storing the data.

2.5.2. Ensure that the individual understands that they can ask for their data to be deleted at any time.

2.5.3. Contact data for individuals that we have not contacted for more than four years will be deleted from the database annually (see part 8)

2.5.4. Refer to the privacy notice for member groups and regular users on the Resource Centre website.

2.6. For group contacts created under point 2.1.7 (unpaid invoice reminders):

2.6.1. This data is stored on the basis of contract. Tick the 'contract' box in the database when storing the data.

2.6.2. When the unpaid invoice has been paid, remove the contact from the group in the database.

2.6.3. Contact details for people who were sent invoice reminders more than four years ago will be deleted from the database annually. (see part 8)

3. Other contact information stored in database

3.1. Group contact details are stored in the database in relation to:

3.1.1. Resource Centre staff members

3.1.2. Resource Centre trustees (if not already stored because they are regular users)

3.1.3. Suppliers

3.1.4. Partner organisations

3.1.5. Funders

3.1.6. Local councillors and council officers

3.2. Check regularly that these contact details are up to date and amend them as required.

3.3. For group contacts created under points 3.1.1 and 3.1.2 (staff and trustees):

3.3.1. This data is stored on the basis of legal obligation. Choose Legal Obligation when adding the data

3.4. For group contacts created under point 3.1.3 (suppliers):

3.4.1. This data is stored on the basis of contract. Tick the 'contract' box when storing the data.

3.5. For group contacts created under points 3.1.4 to 3.1.6 (funders and partner organisations):

3.5.1. This data is stored on the basis of legitimate interest. Tick the 'legitimate interest' box when storing the data.

3.5.2. Contact data for individuals that we have not contacted for more than four years will be deleted from the database annually (see part 8)

4. Contact information stored temporarily on paper forms

4.1. We record contact details on paper forms when:

4.1.1. We take in accounts for examination

4.1.2. We print support session forms

4.2. Check that we have stored contact details in the database, if appropriate (see section 2)

4.3. Ensure that any forms with personal data on are stored properly in files and not left lying around in public areas.

4.4. When the piece of work is finished and has been properly entered up in the database, remove the contact section from the form and shred it before filing.

5. Other personal data stored on paper

5.1. Trustee declaration forms should be filed securely and kept in perpetuity.

5.2. Membership application forms should be kept securely until the next meeting of the Management Committee and then shredded, after the contact details have been entered into the database.

5.3. Names and signatures of people who have been given the wireless password are kept on a sheet at the front desk until the password is changed. When the password changes:

5.3.1. Scan and save the sheet showing the names of people who were given the previous password

5.3.2. Shred the paper record

5.3.3. Delete the previous scanned file

5.4. Printed invoices and Equipment Hire forms should be filed securely

5.5. Personnel records of current staff should be kept securely in the filing cabinet.

5.6. Job application forms and any internal notes relating to recruitment of new staff should be kept securely for 6 months after a new worker is appointed and then shredded.

5.7. Do not store any other paperwork that contains personal data (eg copies of funding applications in group files). If you want to keep something for future use in work with a group, scan it and save it in the electronic file.

5.8. Personnel records of former staff should be kept securely until 6 years after the end of the person's employment, then shredded (but see point 5.9)

5.9. Documents and photographs relating to the history of the Resource Centre may be kept for archival purposes in the public interest. This decision must be made on a case by case basis for

each document. Refer to the Guide to archiving personal data, published by the National Archives[1]. We will only keep personal data in our archive if we consider that:

5.9.1. society as a whole, and in particular researchers, will benefit from preservation of the data for historical research and other purposes

5.9.2. preservation of the data is not likely to cause substantial damage or substantial distress to an individual

6. Personal data contained in emails

6.1. Delete emails from inboxes as soon as they have been dealt with

6.2. Emails will be stored in the Deleted items folders on the front desk computers for 14 days, then permanently deleted automatically.

6.3. All staff should ensure that their own email profile is set up to empty the deleted items folder daily and autoarchive all emails older than 6 months.

6.4. Do not store Contacts in Outlook Address books.

6.5. Suggested contacts (email addresses) are stored in Outlook automatically. Suggested contacts over four years old will be deleted annually (see part 8).

7. Other personal data stored electronically

7.1. Trustee checks are recorded on a spreadsheet which is saved securely on our server and should be kept in perpetuity.

7.2. Job application emails and attachments should be deleted 6 months after a new worker is appointed.

7.3. We store photographs of people using our equipment for publicity purposes. This data is stored on the basis of consent. When we are given a photograph, we should:

7.3.1. Ensure there is a signed photo consent form from the group, scanned and saved in the relevant group folder in the Photos with consent folder.

7.3.2. Delete any photos we are not intending to use for publicity (but see point 5.9).

7.3.3. Delete any photos when we are asked to do so by people who are depicted or by a representative of the group.

7.3.4. When we delete all photos from a group, delete the consent form.

7.4. If people wish to receive an electronic receipt for their card payments from iZettle, they may give us their email address and/or phone number to enter into the card reader. This data is controlled by iZettle. We should ensure that the person understands that their data will be stored by iZettle and may be used to send them a receipt if they use their card to pay any retailer who uses the iZettle system for card payments.

7.5. We use Mailchimp to manage our Friends of the Resource Centre mailing list. This data is stored on the basis of consent.

7.5.1. People who receive Mailchimp mailings from us can unsubscribe using a link in the email.

7.5.2. If anyone contacts us to ask to be removed from one of these mailing lists, we should remove them.

[1] http://www.nationalarchives.gov.uk/documents/information-management/guide-to-archiving-personal-data.pdf

7.5.3. Refer to the Privacy notice for Friends of the Resource Centre on the website.

7.6. Our website uses Cookies to identify users in order to make the booking request feature work properly and in order to analyse usage of our website. Refer to Privacy notice for website users.

7.7. For some suppliers listed on our website, we store and publish personal data. This data is stored on the basis of consent.

7.7.1. When noting or updating supplier details to publish on the website, obtain consent from the supplier and explain that they can ask for their details to be removed at any time.

7.7.2. Record that the supplier has given consent by ticking the box on the website editing screen

7.7.3. Remove suppliers' details on request

Retention periods and routine procedures for deleting data

8. Data that will be deleted daily

8.1. Deleted emails on staff computers. This will happen automatically.

9. Data that will be deleted after 14 days

9.1. Deleted emails on front desk computers. This will happen automatically.

10. Data that will be deleted monthly

10.1. Temporary files, Trash folders, files saved to the Desktop and in the Download folder on all PCs. This is part of the monthly routine of computer maintenance.

11. Data that will be deleted after 6 months

11.1. Sent emails and incoming emails that have been dealt with but not deleted. This will happen automatically.

12. 6 monthly routines

12.1. Delete contacts stored on the Resource Centre's mobile phone if we have not contacted the person by text/Whatsapp for more than 12 months.

13. Annual routines

13.1. Shred paper invoices older than 6 years.

13.2. Shred paper equipment hire forms older than 4 years.

13.3. Delete provisional contacts that have been stored for more than 4 years.

13.4. Delete group contacts stored on the basis of legitimate interest, attached to groups (other than BHCC Tenants' and Residents' Associations) who have not used the Centre for more than 4 years.

13.5. Delete group contacts stored on the basis of legitimate interest and attached to suppliers, funders or partner organisations, if we have not accessed the individual's data for more than 4 years.

13.6. Delete group contacts stored on the basis of consent if we have not accessed the data for more than 4 years.

13.7. Delete group contacts stored on the basis of contract if they are not attached to a group and all invoices they are attached to are older than 4 years.

13.8. Delete all other group contacts that are not attached to a group.

13.9. Delete suggested contacts modified over 4 years ago, in all Outlook profiles.

13.10. Delete electronic documents in Group files and Direct Services files that have not been modified for more than 4 years.

13.11. Remove records stored in Brightpay relating to former employees, if their employment ended more than 6 years ago.

13.12. Shred paper personnel records relating to former employees, if their employment ended more than 6 years ago (but see point 5.9).

13.13. Delete electronic personnel records relating to former employees, if their employment ended more than 6 years ago.

Data protection record-keeping

14. Documentation we keep

14.1. In order to comply with our obligations under the legislation, we will keep the following documents:

14.1.1. Our data audit document

14.1.2. Our data protection policy

14.1.3. Our data protection procedures

14.1.4. Privacy notices for:

i. Users of the Resource Centre website

ii. Friends of the Resource Centre

iii. Donors to the Resource Centre

iv. Users of the equipment hire service

v. Resource Centre members and regular users

14.1.5. Records in the database showing the basis on which personal data is held and the date it was last accessed. This includes records of consent having been given, where applicable.

14.1.6. Records on the website showing consent to publish personal data of suppliers

14.1.7. Records of any data breaches

14.2. These documents will be kept up to date and reviewed every two years.

15. In case of a data breach

15.1. Take all reasonable steps to recover any data that has been lost, stolen or shared in error, and to minimise the impact on individuals' privacy.

15.2. Keep notes of your actions.

15.3. Report the issue to the rest of the workers' group.

15.4. The workers' group will

15.4.1. Evaluate what happened and make any necessary changes to our procedures.

15.4.2. Decide whether it is necessary to report the breach to the ICO.