# Data Protection Policy

# Barking & Dagenham Renew

# Definitions

| | |
|---|---|
| **Charity** | means Barking & Dagenham Renew, a registered charity. |
| **GDPR** | means the General Data Protection Regulation. |
| **Responsible Person** | means the current Trust Officer. |
| **Register of Systems** | means a register of all systems or contexts in which personal data is processed by the Charity. |

## 1. Data protection principles

The Charity is committed to processing data in accordance with its responsibilities under the GDPR.

Article 5 of the GDPR requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;
b. 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;
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d. 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;
e. 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
f. 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."

## 2. General provisions

a. This policy applies to all personal data processed by the Charity.
b. The Responsible Person shall take responsibility for the Charity's ongoing compliance with this policy.
c. This policy shall be reviewed at least annually.

d. The Charity shall register with the Information Commissioner's Office as an organisation that processes personal data.

## 3. Lawful, fair and transparent processing

a. To ensure its processing of data is lawful, fair and transparent, the Charity shall maintain a Register of Systems.
b. The Register of Systems shall be reviewed at least annually.
c. Individuals have the right to access their personal data and any such requests made to the charity shall be dealt with in a timely manner.

## 4. Lawful purposes

a. All data processed by the charity 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).
b. The Charity shall note the appropriate lawful basis in the Register of Systems.
c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
d. 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 Charity's systems.

## 5. Data minimisation

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

## 6. Accuracy

a. The Charity shall take reasonable steps to ensure personal data is accurate.
b. 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.

## 7. Archiving / removal

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

## 8. Security

a. The Charity shall ensure that personal data is stored securely using modern software that is kept-up-to-date.
b. 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.
c. When personal data is deleted this should be done safely such that the data is

irrecoverable.

d. Appropriate back-up and disaster recovery solutions shall be in place.

## 9. 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 Charity 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).

# Register of Systems

## The data we collect and in what way

- We collect contact information of people who get in touch with the Charity. This will be their basic information, such as their name, email address, phone number, and work address. It would be nothing more than what was shared with us in their email signature.

  This information is inputted to Zoho CRM by the Trust Officer.

  Personal data for individuals who make contact with us is processed on the basis of legitimate interest.

- In addition to their contact information, grant applicants are required to give a bit more information about themselves. Given the nature of the work being funded, these applications could contain information related to employment status, previous work history, or medical diagnoses.

  Applications are written down on a word document which is stored on Zoho Docs. Once this has been approved by the applicant, it is then inputted to Zoho CRM by the Trust Officer.

  The data of grant applicants is processed using consent, obtained from them during their application.

- Successful applicants are required to give us bank details to allow for a money transfer. This may be a personal bank account.

  This information is inputted to Zoho CRM by the Trust Officer.

- To help inform our work, we will gather information for the purpose of equality monitoring. This will be gathered by consent using an anonymised online form as part of the application process.

  This data will be stored on Zoho Survey and used in annual reports.

- From time to time, we may produce other surveys along with partner organisations, again using Zoho Surveys. These surveys may ask for personal information such as name and contact details if we require future contact.

  Any personal data given through a survey will only be used to contact you in relation to that survey and will be deleted when it is no longer needed.

  Only anonymised data from these surveys will be shared with partners through reports.

**How the data is stored and who has access to it**

All data is stored using Zoho software.

- Zoho CRM is used to store all the data mentioned above.
- Zoho Survey is used to store all data gathered through surveys.
- Zoho Docs is used to store all of the Charity's documentation in a secure location. This a cloud-based storage software which is accessible through a browser or a desktop application.

The software can currently only be accessed by the Trust Officer and is protected using 2-factor authentication (2FA), meaning that access to the information requires not only the Trust Officer's log-in details but their phone as well.

Any future staff members would have the same 2FA process in place. Additionally, the Zoho software allows for data to be restricted according to role, a feature which would be used as the organisation expands.

Zoho software contains an auditing feature which will show exactly who has accessed data and what they have done with it.

**Sharing the data**

- The whole data set is only accessible by the Trust Officer, unless access is legally required by a third party.

- Application data is shared with the board of Trustees on a monthly basis to allow them to make their funding decisions. They are sent the written applications via email, with the consent of the applicants.

- Contact data will only be shared with others with the permission of the person whose data is being requested.

- Anonymised monitoring data is shared with the board of Trustees at an annual review, and would also be shared with any funders who require this of us as part of a funding agreement.

**Purpose for which the data is used**

- Personal data related to applications will be used to contact people in relation to their application.
- Personal data related to surveys will be used to contact people for the reasons laid out in a specific survey.

**Data removal and archiving**

- On Zoho CRM, Application data is stored separately from Contact/Applicant data.

  The Charity needs to retain the Application data to be able to carry out its work. As some of the Applications could contain personal information, as indicated above, this data will be reviewed annually to see if all of the data is still needed.

Any and all personal data can be removed from the CRM with ease. Single data entries can be removed immediately but whole Applicant profiles are stored in a Recycle Bin for 60 days before being permanently deleted. This is to ensure that accidentally deleted information can be recovered but purposefully deleted records will not be retrieved from the Recycle Bin. Any retrieval would be shown on the audit log mentioned above.

- Personal data which is stored on Zoho Docs can be removed immediately but, again, the files are kept in a Recycle Bin for 60 days before being permanently deleted.