Dorcas Befriending Project

Information & Data Protection Policy

Contents:

The Bridge, 80 Arran Walk,
Marquess Estate,
Canonbury, Islington, London N1 2TL
020 7704 0605

Subject Access

- Responsibility
- Procedure for making requests
- Provision for verifying identity
- Charging
- Procedure for Granting Access

Transparency

- Commitment
- Procedure
- Responsibility

Consent

Direct Marketing

Policy Review

The Bridge, 80 Arran Walk,
Marquess Estate,
Canonbury, Islington, London N1 2TL
020 7704 0605

Information & Data Protection Policy of the Dorcas Befriending Project

Policy Purpose

The aim of this policy is to ensure that the Dorcas Befriending Project (DBP) is in compliance with the 1998 Data Protection Act and protects individuals and the charity organisation from the following primary risks:

- Information about individuals getting into the wrong hands, through poor security or inappropriate disclosure of information
- Individuals being harmed through data being inaccurate or insufficient
- Information being needlessly withheld
- Accidental loss or damage of confidential data

Introduction to the Data Protection Act

The 1998 Data Protection Act regulates the collection, storage use and disclosure of information by organisations about individuals. Any organisation that keeps information about individuals must comply with the Act. Failure to comply with the Act could result in loss of reputation as well as potential penalties from The Information Commissioner's Office that has the authority to issue fines of up to £500,000 and prison sentences.

Note – The Act applies to personal data, that is defined as information about identifiable living individuals that is:

- Held on a computer or any other automated system
- Held in a relevant filing system
- Intended to go onto a computer or into a relevant filing system

Data Protection Principles

Whenever collecting information about people, the DBP agrees to apply the following Eight Data Protection Principles:

1. Personal data must be processed fairly and lawfully
2. Personal data must be obtained only for the purpose(s) specified
3. Data must be adequate, relevant and not excessive for the purpose(s) required
4. Data must be accurate and kept up-to-date
5. Data must not be kept for longer than is necessary for the required purpose(s)
6. Data subjects rights must be respected
7. Appropriate technical and organisational measures must be taken to prevent unauthorised or unlawful processing of personal data and to protect against accidental loss or destruction or damage to personal data
8. Personal data shall not be transferred outside the European Economic Area (EEA) unless that country or territory ensures an adequate level of data protection

The Bridge, 80 Arran Walk,
Marquess Estate,
Canonbury, Islington, London N1 2TL
020 7704 0605

Policy Statement

The DBP is committed to:

- Complying with both the law and industry best practice
- Respecting individuals' rights
- Being open and honest with individuals whose data is held, and allow them to see their data within the legal limit of 40 days after an access request has been submitted
- Providing training and support for staff and volunteers who handle personal data, so that they can act confidently and consistently
- Notifying the Information Commissioner's Office voluntarily
- Taking steps to ensure personal data is protected

Responsibilities

- The **Executive Committee** has the overall responsibility of ensuring that the organisation complies with its legal obligations
- The **Data Protection Officer** is responsible for:
    - Reviewing Data Protection and related policies
    - Advising other staff on tricky Data Protection issues
    - Ensuring that Data Protection induction and training takes place
    - Notification – completing the form for the Information Commissioner and paying the annual fee (a direct debit has been set up to automatically renew every year)
    - Handling subject access requests
    - Approving unusual or controversial disclosures of personal data
    - Approving contracts with Data Processors should work be outsourced
    - Managing electronic security
    - Approving Data-Protection-related statements on publicity materials, letters, etc
- All **Staff & Volunteers** are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work

Confidentiality

Scope: Confidentiality applies to a much wider range of information than Data Protection. Examples of information that is likely to be confidential, but may well not be subject to Data Protection, include:

- Information about the organisation and its plans or finances
- Information about other organisations, since Data Protection only applies to information about individuals
- Information which is not recorded, either on paper or electronically
- Information held on paper, but in a sufficiently unstructured way that it does not meet the definition of a "relevant filing system" in the Data Protection Act

Accordingly, the DBP is committed to applying appropriate confidentiality to all the information it handles.

The Bridge, 80 Arran Walk,
Marquess Estate,
Canonbury, Islington, London N1 2TL
020 7704 0605

Understanding Confidentiality: Normal access is defined as appropriate on a "need to know" basis for this purpose; no one should have access to information unless it is relevant to his or her work. This may be relaxed in the case of information which poses a low risk: for example a list of industry contacts may be made generally available, even if this means people having access who don't strictly need it. Notably, the Executive Committee and volunteers must treat all confidential information disclosed (deliberately or accidentally) by clients during the normal course of befriending interactions in the strictest confidence unless a situation arises where the recipient of the information is reasonably concerned or aware of a genuine risk to the client, his or her own wellbeing, the charity or community. In such a situation of risk, or when in doubt, the volunteer, staff or member should refer to the Project Coordinator or Executive Committee for further attention. Such situations will be handled on a case-by-case basis as appropriate.

Communication with Data Subjects: Confidentiality statements are to be clearly presented on all forms, correspondence and at the point of collection of data stating why the information is being obtained, to whom it is relevant and how it will be used and stored. Individuals have a right to see what data is kept on them, and for what purpose within 40 days of a written request.

Communication with Volunteers and Staff: Volunteers and staff will be informed and trained in their responsibilities as part of their induction. Should they have any subsequent questions about whether information should be disclosed, or access allowed, the first point of reference should be the Project Coordinator or the Executive Committee.

Authorization for disclosure not directly related to the reason why data is held: These fall into two main categories: those likely to be at the instigation, or in the interests, of the Data Subject, and those which are made in the course of official investigations. For the first (such as a reference request for a volunteer or staff member), consent from the Data Subject is sufficient authorization. This consent must be recorded in writing. For the second, the Data Subject may not be informed, as appropriate; authorization will be made at the Executive Committee level.

Security

The DBP has adopted the following information security policy to guard against unauthorised or unlawful processing of personal data and against accidental loss, destruction or damage:

- Control physical security of data by keeping all project and individual records in a locked filing cabinet in a secure location
- Place password controls on access to information on both electronic file and computer level
- Take regular back-ups of computer data files and store these back-ups in safe, separate locations
- Train all staff on security systems and procedures

The Bridge, 80 Arran Walk,
Marquess Estate,
Canonbury, Islington, London N1 2TL
020 7704 0605

- Detect and investigate breaches of security should they occur
- Should individuals work from home, they must agree to keep work secure and to return all work related materials and to remove from their personal computers any records once a project is complete. Furthermore, they should inform the organisation if information gets into the wrong hands.

Data Recording & Storage

Every effort will be made to maintain the accuracy of all data recorded.
All records will be kept as up to date and consistent as possible.
All records will be stored securely and backed up regularly.
Records will not be kept longer than is absolutely necessary.
Archives will be maintained for up to 3 years, or longer if necessary.

Subject Access

The Data Protection Officer will respond to all requests for personal data by the Subject.
These requests must be made in writing, and the data provided to the subject within 40 days of this request, as is legally required.
Should the Data Protection Officer not know the Subject personally, identification must be verified through photographic evidence.
Once the Subject's identity has been confirmed, the Data Protection Officer may communicate the information to the Subject as appropriate.
No charge will be taken for providing data to Subjects.

Transparency

The DBP is committed to transparency on all levels of the organisation.
Should any questions be raised, they will be addressed as soon as possible.
The responsibility of ensuring transparency across the organisation rests with all Executive Committee.

Consent

The DBP will accept written consent authorizing the use of personal data. Alternatively, verbal consent will also be accepted if it is documented in meeting minutes.

The DBP will provide individuals the opportunity to opt out of their data being used in particular ways. Subjects may make their intention known on their initial application form or in written or documented verbal form.

The Bridge, 80 Arran Walk,
Marquess Estate,
Canonbury, Islington, London N1 2TL
020 7704 0605

The DBP acknowledges that, once given, consent can be withdrawn, but not retrospectively. There may be occasions where the DBP must retain data for a certain length of time, even though consent for using it has been withdrawn.

Direct Marketing

The DBP will not release information on volunteers or clients for direct marketing purposes.

Policy Review

This policy will be reviewed by the Executive Committee every three years or as required.

Author(s):	Zakari Momodu & Amy Shearer
Approved by:	Executive Committee
Date Accepted:	26 January 2013

The Bridge, 80 Arran Walk,
Marquess Estate,
Canonbury, Islington, London N1 2TL
020 7704 0605