



CONFIDENTIALITY POLICY

Contents

1. General Principles
2. What Information is Held
3. Access to Information
4. Storing Information
5. Duty to Disclose
6. Disclosures
7. Data Protection Act
8. Breach of Confidentiality
9. Whistle Blowing

The Dorcas Befriending Project (DBP) takes the confidentiality of clients and volunteers very seriously. The DBP recognises that it has a legal and moral obligation to uphold the confidentiality of all clients, staff and volunteers.

General principles

A confidentiality policy is necessary to protect clients, staff and volunteers and the Executive Committee from the possibility of information about them being passed on to individuals or organisations that have no right to that information. It is also important to provide guidance to staff and volunteers on the extent to which confidentiality is to be preserved, circumstances in which it may be breached, and measures to be taken in either eventuality.

The DBP recognises that the Executive Committee, volunteers and staff gain information about individuals and organisations during the course of their work or activities. In most cases such information will not be stated as confidential and colleagues may have to exercise common sense and discretion in identifying whether information is expected to be confidential. This policy aims to give guidance but if in doubt, seek advice from the Project Co-ordinator and/or member of the Executive Committee.

Volunteers and staff are able to share information with the Project Co-ordinator and the Executive Committee in order to discuss issues and seek advice.

The Executive Committee, volunteers and staff will avoid exchanging personal information or comments about individuals with whom they have a professional relationship, without a specific requirement to do so.

Volunteers and staff will not disclose to anyone, other than the Project Co-ordinator and/or appropriate member of the Executive Committee, any information considered sensitive, personal, financial or private without the knowledge or consent of the individual or an officer, in the case of an organisation without good reason to do so.

The Executive Committee, volunteers and staff will avoid talking about organisations or individuals in social settings.

There may be circumstances where the Executive Committee, volunteers and staff would want to discuss difficult situations with each other to gain a wider perspective on how to approach a problem. Consent must be sought before discussing the situation as appropriate. Alternatively, a discussion may take place with names or identifying information remaining confidential.

Where there is a legal duty on the DBP to disclose information, the person to whom the confidentiality is owed will be informed that disclosure has or will be made.

Why information is held

Most information held by the DBP relates to individuals, voluntary and community organisations, self-help groups, volunteers, students, staff, trustees or services which work with, support or fund them.

Information is kept to enable the DBP's Executive Committee, volunteers and staff to understand the history and activities of individuals or organisations in order to deliver the most appropriate services.

The DBP has a role in putting people in touch with voluntary and community organisations and keeps contact details which are passed on to any enquirer, except where the group or organisation expressly requests that the details remain confidential.

Information about ethnicity and disability of users is kept for the purposes of monitoring our equal opportunities policy and also for reporting back to funders and research purposes.

Access to information

Information is confidential to the DBP as an organisation and will only be passed to the Executive Committee, volunteers and staff on a need to know basis to ensure the best quality service for clients.

Where information is sensitive, i.e. it involves disputes or legal issues; it will be confidential to the Executive Committee member and/ or employee dealing with the case. Such information should be clearly labelled 'Confidential' and should state the names of those entitled to access the information and the name of the individual or group who may request access to the information.

Members may have sight of the DBP's records held in their name or that of their organisation. The request must be in writing to the Secretary giving 14 days' notice and be signed by the individual, or in the case of an organisation's records, by an Executive Officer. Sensitive information will only be made available to the person or organisation named on the file.

When photocopying or working on confidential documents, the Executive Committee, volunteers and staff must ensure people passing do not see them. This also applies to information on computer screens.

Storing Information

General non-confidential information about organisations is kept in a filing cabinet, online and in computer files.

Personnel information on staff, volunteers, and other individuals working within the DBP will be kept in lockable filing cabinets, by the Executive Committee. Personnel information may also be held in computer files that are password protected.

Files or filing cabinet drawers bearing confidential information should be labelled 'confidential'.

In an emergency situation, the Executive Committee may authorise access to files by other people.

Duty to Disclose Information

There is a legal duty to disclose some information including:

Any form of abuse or criminal activity will be reported to the appropriate authority.

In addition members' believing an illegal act has taken place, or that a client is at risk of harming themselves or others, must report this to the Project Co-ordinator and/or Safeguarding leads who will report it to the appropriate authorities.

Clients should be informed of any disclosures.

Disclosures

The DBP complies fully with the DBS (Disclosure and Barring Service – previously CRB) code of practice regarding the correct handling, use, storage, retention and disposal of Disclosures and Disclosure information.

Disclosure information is always kept separately from an applicant's personnel file in secure storage with access limited to those who are entitled to see it as part of their duties. It is a **criminal offence** to pass this information to anyone who is not entitled to receive it. Documents will be destroyed by secure means. Photocopies will not be kept. However, the DBP will keep a record of the date of issue of a Disclosure, the name of the subject, the type of Disclosure requested, the position for which the Disclosure was requested, the unique reference number of the Disclosure and the details of the recruitment decision taken.

Data Protection Act

Information about individuals, whether on computer or on paper, falls within the scope of the Data Protection Act and will be held in accordance with our Data Protection policy available on the DBP's website <http://dorcas-befriending.org.uk/what-we-do/dbp-policies/>

Breach of Confidentiality

Members who are dissatisfied with the conduct or actions of other members or the DBP in relation to confidentiality should raise this with the Executive Committee using the Complaints and Grievance Procedure outlined in the Complaints Policy, if necessary, and are asked not discuss their dissatisfaction outside of the DBP.

Members accessing unauthorised files or breaching confidentially may face disciplinary action.

Whistle blowing

Where a member has concerns about any matter (e.g. the use of the DBP funds), he or she may refer directly to the Chair or Treasurer outside the usual complaints procedure.

All members hold the right to inform either the Project Co-ordinator or a member of the Executive Committee if they believe that the DBP is being brought into disrepute by the actions of another member.

Author(s):	Kelly Rowley
Approved by:	Executive Committee
Date Accepted:	26 January 2013