# DUMFRIES AND GALLOWAY BEFRIENDING PROJECT

# PRIVACY POLICY

**October 2018**

## Contents

## 1. Introduction

Dumfries and Galloway Befriending Project (DGBP) ("we" or "us") is committed to ensuring the secure and safe management of data held by us in relation to young people, befrienders, staff and other individuals. Our staff members have a responsibility to ensure compliance with the terms of this policy, and to manage individuals' data in accordance with the procedures outlined in this policy and documentation referred to herein.

We need to gather and use certain information and manage a significant amount of data, from a variety of sources. This data contains "personal data" and "sensitive personal data" (known as "special categories of personal data" under the GDPR).

This policy sets out our duties in processing that data, and the purpose of this policy is to set out the procedures for the management of such data.

## 2. Legislation

It is a legal requirement that we process data correctly; we must collect, handle and store personal information in accordance with the relevant legislation.

The relevant legislation in relation to the processing of data is:

(a) the General Data Protection Regulation (EU) 2016/679 (the GDPR);

(b) the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications); and

(c) any legislation that, in respect of the United Kingdom (UK), replaces, or enacts into UK domestic law, the General Data Protection Regulation (EU) 2016/679, the proposed Regulation on Privacy and Electronic Communications or any other law relating to data protection, the processing of personal data and privacy as a consequence of the UK leaving the European Union.

## 3. Data

Personal data is that from which a living individual can be identified either by that data alone, or in conjunction with other data held by us.

DGBP holds information of various types which fall within the definition of "personal data". The most significant is data regarding volunteer befrienders and young people (the users of its services). This includes:

(a) basic information collected upon application and referral, and correspondence relating to appointments.

(b) case notes made by the Volunteer Co-ordinators, following progress meetings.

DGBP tries to ensure that people whose personal data is being collected are aware that this information is being recorded and held, and that they consent to the collection, retention and use of that information. The Project will also endeavour to ensure that the information held is no more than the minimum required and is accurate.

DGBP is aided in the above by the fact that, in the case of the volunteer befrienders, most data is provided by them rather than by third parties and, in the case of the young people, they too are privy to the application form and complete a section of it themselves.

The Referral Form is designed to collect and record only that information which is essential to ascertain the young person's wishes regarding the future befriending match.

DGBP recognises that some of this information will be 'sensitive' as defined in the Act, in so far as it relates to Racial or Ethnic Origin, Political Opinions, Religious Beliefs or similar, Physical or Mental Health, and Criminal Proceedings or Convictions. It also recognises that it has responsibilities regarding the use of this information.

## 4. Processing of personal data

4.1 We are permitted to process personal data on behalf of data subjects provided it is doing so on one of the following grounds:

- processing with the consent of the data subject;
- processing is necessary for the performance of a working agreement between us and the data subject or for entering into a working agreement with the data subject;
- processing is necessary for our compliance with a legal obligation;
- processing is necessary to protect the vital interests of the data subject or another person; or
- processing is necessary for the purposes of legitimate interests.

4.2 GDPR notice

- We have produced a GDPR notice which we are required to provide to all parties whose personal data is held by us. That notice must be provided from the outset of processing their personal data and they should be advised of the terms of the notice when it is provided to them.

- The notice at Appendix 1 sets out the personal data processed by us and the basis for that processing.

4.3 Employees

Employee personal data is held and processed by us. A copy of any employee's personal data held by us is available upon written request by that employee from Mr Alex Dickson, Project Manager.

4.4 Consent

Consent as a ground of processing will require to be used from time to time by us when processing personal data. It should be used by us where no other alternative ground for processing is available. In the event that we require to obtain consent to process a data subject's personal data, we shall obtain that consent in writing. The consent provided by the data subject must be freely given and the data subject will be required to sign a relevant consent form if willing to consent. Any consent to be obtained by us must be for a specific and defined purpose (i.e. general consent cannot be sought).

4.5 Processing of special category personal data or sensitive personal data

In the event that we process special category personal data or sensitive personal data, we must do so in accordance with one of the following grounds of processing:

- the data subject has given explicit consent to the processing of this data for a specified purpose;
- processing is necessary for carrying out obligations or exercising rights related to employment or social security;
- processing is necessary to protect the vital interest of the data subject or, if the data subject is incapable of giving consent, the vital interests of another person;
- processing is necessary for the establishment, exercise or defence of legal claims, or whenever courts are acting in their judicial capacity; and
- processing is necessary for reasons of substantial public interest.

**5. Data sharing**

5.1 We share our data with third-parties in order that day to day activities are carried out in accordance with our relevant policies and procedures. In order that we can monitor compliance by these third-parties with data protection laws, we will require the third-party organisations to enter in to a working agreement with us to govern the processing of data, security measures to be implemented and responsibility for breaches.

5.2 Personal data is from time to time shared amongst us and third-parties who require to process personal data that we process as well. We and the third-party will be processing that data in their individual capacities as data controllers (e.g. for processing of the employees' pension).

5.3 Data processors

A data processor is a third-party entity that processes personal data on behalf of us and are frequently engaged if certain parts of our work is outsourced (e.g. payroll). A data processor must comply with data protection laws. Our data processors must ensure they have appropriate technical security measures in place, maintain records of processing activities and notify us if a data breach is suffered. If a data processor wishes to sub-contact their

processing, our prior written consent must be obtained. Upon a sub-contracting of processing, the data processor will be liable in full for the data protection breaches of their sub-contractors.

## 6 Data storage, security and confidentiality

All personal data held by us must be stored securely, whether electronically or in paper format.

6.1 Paper storage

If personal data is stored on paper it should be kept in a secure place where unauthorised personnel cannot access it. Employees should make sure that no personal data is left where unauthorised personnel can access it. When the personal data is no longer required it must be disposed of by the employee so as to ensure its destruction. If the personal data requires to be retained on a physical file then the employee should ensure that it is properly secured within the file which is then stored in accordance with our storage provisions.

6.2 Electronic storage

Personal data stored electronically must also be protected from unauthorised use and access. Personal data should be password protected when being sent internally or externally to our data processors or those with whom we have entered in to a data sharing agreement. If personal data is stored on removable media (CD, DVD, USB memory stick) then that removable media must be stored securely at all times when not being used.

6.3 Confidentiality

DGBP has produced policy documents setting out principles and practice relating to confidentiality. It states "information on children and young people referred to the Project and volunteer befrienders is kept confidential to the Project and is shared only between Project staff and the agent referring to the Project, on a need-to-know basis".

It goes on to state that "in exceptional circumstances – when the child and young person involved, or a young person known to them, is perceived to be at risk of significant harm – the information may be shared out with this circle on a strictly 'need to know' basis". All Befrienders and Project staff will receive a copy of the policy documents and will be required to sign a declaration of confidentiality, a copy of which is retained in their personal files.

## 7 Breaches

7.1 A data breach can occur at any point when handling personal data and we have reporting duties in the event of a data breach or potential breach occurring. Breaches which pose a risk to the rights and freedoms of the data

subjects who are the subject of the breach require to be reported externally in accordance with clause 7.3 hereof.

7.2 Internal reporting

We take the security of data very seriously and in the unlikely event of a breach will take the following steps:

- As soon as the breach or potential breach has been identified, and in any event no later than six (6) working hours after it has been identified, Mr Alex Dickson must be notified in writing of (i) the breach; (ii) how it occurred; and (iii) what the likely impact of that breach is on any data subject(s);
- we must seek to contain the breach by whatever means available;
- we must consider whether the breach is one which requires to be reported to the Information Commissioner's Office (ICO) and data subjects affected and do so in accordance with this clause 7;
- notify third parties in accordance with the terms of any applicable data sharing agreements

7.3 Reporting to the ICO

We are required to report any breaches which pose a risk to the rights and freedoms of the data subjects who are the subject of the breach to the ICO within 72 hours of the breach occurring. We must also consider whether it is appropriate to notify those data subjects affected by the breach.

## 8 Data subject rights

8.1 Certain rights are provided to data subjects under the GDPR. Data subjects are entitled to view the personal data held about them by us, whether in written or electronic form.

8.2 Data subjects have a right to request a restriction of processing their data, a right to be forgotten and a right to object to our processing of their data.

8.3 Subject access requests

Data subjects are permitted to view their data held by us upon making a request to do so (a subject access request). Upon receipt of a request by a data subject, we must respond to the subject access request within one month of the date of receipt of the request.

We:

8.3.1. must provide the data subject with an electronic or hard copy of the personal data requested, unless any exemption to the provision of that data applies in law;

8.3.2. where the personal data comprises data relating to other Data subjects, must take reasonable steps to obtain consent from those data subjects to the disclosure of that personal data to the data subject who has made the subject access request

8.3.3. where we do not hold the personal data sought by the data subject, must confirm that we do not hold any personal data sought by the data subject as soon as practicably possible, and in any event, not later than one month from the date on which the request was made.

8.4 DGBP has a written policy and procedures under which befrienders and young people have access to their own personal files.

8.4.1 The procedure for young people begins with a written request to the Project Manager.

8.4.2 Information given in confidence by a third party can only be accessed with written permission from the relevant person.

8.4.3 Volunteer befrienders are advised, at the interview stage, that they may read their personal profile then if they so wish. Also, referrers may read a summarised profile of the befriender's file, in confidence, prior to matching. Subsequent access to their file by a befriender must be by written request to the Project Manager.

8.4.5 The policy and procedures are in line with the terms of the Access to Personal Files Act, 1987.

8.5 The right to be forgotten

8.5.1 A data subject can exercise their right to be forgotten by submitting a request in writing to us seeking that we erase the data subject's personal data in its entirety.

8.5.2 Each request received by us will require to be considered on its own merits and legal advice will require to be obtained in relation to such requests from time to time. We have responsibility for accepting or refusing the data subject's request in accordance with this clause and will respond in writing to the request.

8.6 The right to restrict or object to processing

8.6.1 A data subject may request that we restrict our processing of the data subject's personal data, or object to the processing of that data.
In the event that any direct marketing is undertaken from time to time by us, a data subject has an absolute right to object to processing of this nature by us, and if we receive a written request to cease processing for this purpose, then we must do so immediately.

8.6.2 Each request received by us will require to be considered on its own merits and legal advice will require to be obtained in relation to such requests from time to time. We have responsibility for accepting or refusing the data subject's request in accordance with clause 8.6 and will respond in writing to the request.

## 9 Privacy impact assessments

Privacy impact assessments (PIAs) are a means of assisting us in identifying and reducing the risks that our operations have on personal privacy of data subjects.

9.1 We shall:

9.1.1 Carry out a PIA before undertaking a project or processing activity which poses a high risk to an individual's privacy. High risk can include, but is not limited to, activities using information relating to health or race, or the implementation of a new IT system for storing and accessing personal data.

9.1.2 In carrying out a PIA, include a description of the processing activity, its purpose, an assessment of the need for the processing, a summary of the risks identified and the measures that we will take to reduce those risks, and details of any security measures that require to be taken to protect the personal data.

9.2 We will require to consult the ICO in the event that a PIA identifies a high level of risk which cannot be reduced. We will be responsible for such reporting, and where a high level of risk is identified by those carrying out the PIA they require to notify us within five (5) working days.

## 10 Archiving, retention and destruction of data

As a voluntary organisation there are no 'legal requirements' regarding the length of time to keep 'personal' files. There is, however, a legal requirement to keep financial information for 7 years.

We review our data retention periods regularly and will only hold your personal data for as long as is necessary for the relevant activity, or as required by law.

When a young person or befriender leaves the Project computer records will be kept to show:

10.1 Whose file was destroyed (only name, date of birth, gender and contact details of the young person or befriender, referral agency, reason for ending match, start and end dates of match and GIRFEC score data will be retained)

10.2 how the file was destroyed

10.3 when it was destroyed

10.4 who authorised the destruction

10.5 with whom matched

To give time for all procedures to be completed, records will be kept for up to 12 months.

Personal files of the befriender/young person will be reviewed 6 months after finishing with the Project. If applicable, records will be destroyed.

Young persons' files may be kept for a further 6 month period to allow any query relating to a terminated match to be investigated.

Files can also be kept for another 6 months, which will allow time for volunteers to take a break, if they wish, between befriending matches. Volunteers who had indicated they were taking a temporary break from befriending will be contacted to clarify their future commitment to befriending. Records may then be kept on the instruction of an individual volunteer for the next 6 month period and at the end of this time records will be destroyed if the volunteer is not able to commit to befriending at this time.

The Project will use 31st December and 30th June each year as end dates to destroy files of befriending matches terminated during the 12 month period.

Files will be destroyed by cross cut shredding. Records kept on the computer will be deleted. Basic database information will be kept as statistical records.

**List of appendices**

1. GDPR Notice

**Dumfries & Galloway Befriending Project**
**19 Bank Street, Dumfries DG1 2NX**
**Tel – 01387 247812 www.befriending.org**
**Email – projectoffice@befriending.org**

# GDPR Notice

**(How we use your personal information)**

This notice explains what information we collect, when we collect it and how we use this. During the course of our activities we will process personal data (which may be held on paper, electronically, or otherwise) about you and we recognise the need to treat it in an appropriate and lawful manner. The purpose of this notice is to make you aware of how we will handle your information.

Dumfries & Galloway Befriending Project ("**we**" or "**us**") take the issue of security and data protection very seriously and strictly adhere to guidelines published in the Data Protection Act of 1998 and the General Data Protection Regulation (EU) 2016/679 which is applicable from the 25 May 2018, together with any domestic laws subsequently enacted.

We are notified as a data controller with the Information Commissioner's Office (ICO) under registration number Z5014962 and we are the data controller of any personal data that you provide to us.

Any questions relating to this notice and our privacy practices should be sent to Mr Alex Dickson, 19 Bank Street, Dumfries, DG1 2NX, projectoffice@befriending.org

## How we collect information from you and what information we collect

We collect information about you:

- when you engage with us,
- when we carry out our processes,
- from your arrangements to make payment to us or for us to make payment to you (such as bank details),

We collect the following information about you:

- Name;
- Address;
- Telephone number;
- email address;
- Date of birth;
- Principal bank account details, if relevant.

**Why we need this information about you and how it will be used**

We need your information and will use your information:

- to undertake management and administration of DGBP and its services;
- to provide and monitor matches between volunteer befrienders and young people;
- for research and forward planning purposes;
- for awareness raising and to send you details of any changes which may affect you;

**Sharing of your information**

The information you provide to us will be treated by us as confidential and will be processed only by us. Unless required to do so by law, we will not share, sell or distribute any of the information you provide to us without your consent.

**Security**

When you give us information we take steps to make sure that your personal information is kept secure and safe. All the personal data held by DGBP is kept at its office in Dumfries. Paper files are kept in locked cabinets to which only Project staff have access. Access to computers is by password, known only to staff.

When volunteer befrienders commence a match, they will be issued with a notebook in which they may wish to record appropriate information. In these circumstances, befrienders are advised to keep these notes in a secure place.

**Your rights**

You have the right at any time to:

- ask for a copy of the information about you held by us in our records;
- require us to correct any inaccuracies in your information;
- make a request to us to delete what personal data we hold about you; and
- object to receiving any marketing communications from us.

If you would like to exercise any of your rights above please contact us at projectoffice@befriending.org Should you wish to complain about the use of your information, we would ask that you contact us to resolve this matter in the first instance. You also have the right to complain to the Information Commissioner's Office (ICO) in relation to our use of your information. The ICO's contact details are noted below:

The Information Commissioner's Office – Scotland
45 Melville Street, Edinburgh, EH3 7HL
Telephone: 0131 244 9001
email:scotland@ico.org.uk

The accuracy of your information is important to us - please help us keep our records updated by informing us of any changes to your email address and other contact details.