Derby City Centre Chaplaincy: Data Protection Policy 2020

Purpose of this policy
Personal information stored or processed on a computer is subject to the Data Protection Act 1998 (DPA) and, from 25 May 2018, the General Data Protection Regulation (GDPR), which came about because of the growth of the "Information Society" in particular, in response to concerns about the threat to personal privacy that the manipulation and transfer of data by computers can pose.

Derby City Centre Chaplaincy (DCCC) is committed to ensuring that it holds and processes personal data in full compliance with the DPA and GDPR and acknowledges that breaking the DPA/GDPR contravenes the law and may result in DCCC being prosecuted, fined and/or our reputation being damaged.

DCCC is exempt from registration with the Information Commissioner on the basis that we:

- are established for not-for-profit making purposes and do not make a profit to enrich others;
- only process information necessary to establish or maintain membership or support;
- only process information necessary to provide or administer activities for people who are members of the organisation or have regular contact with it;
- only share the information with people and organisations necessary to carry out the DCCC's activities and only with permission to share information from the data subject; and
- only keep the information while the individual is a beneficiary, member or supporter or as long as necessary.

Should any of the above cease to be the case we will register with the Information Commissioner in line with his/her requirements.

Requirements of the DPA/GDPR
The people about whom we hold information are referred to in this policy as data subjects.

Under the DPA/GDPR, any personal data, including that held on electronic or manual filing systems, must:

- be processed fairly, lawfully and in a transparent manner,
- be collected for specific, explicit and legitimate purposes,
- be adequate, relevant and limited to what is necessary,
- be accurate and kept up to date,
- be processed and stored securely and in accordance with the data subject's rights,
- not be kept longer than is necessary and
- not be transferred outside the European Economic Area (EEA) unless strict conditions are met in accordance with the requirements of GDPR.

Processing personal data is only lawful if:

- the data subject has given consent for one or more specific purposes,
- it is necessary to meet contractual obligations entered into by the data subject,

- it is necessary to comply with legal obligations of DCCC (as data controller),
- it is necessary to protect the vital interests of the data subject,
- it is necessary to necessary for tasks in the public interest or the exercise of authority vested in DCCC (as data controller), or
- it is for the purposes of legitimate interest pursued by DCCC (as data controller),

Consent from a data subject (where required) must:

- be clearly given, intelligible and easily accessible and
- able to be withdrawn at any time in a manner as easy as it was to give.

Anyone under the age of 16 is not legally able to give consent and parental authorisation is instead required.

Data subjects have rights regarding the processing of personal data including rights to:

- access their data and information about its uses;
- have their data corrected or completed;
- have their data erased if:
  - the data is no longer necessary in relation to the purposes for which they were collected;
  - they withdraw their consent and there is no other lawful basis for processing the data;
  - they object to the processing and there are no overriding legitimate grounds for the processing;
  - it has been unlawfully processed and
  - it has to be erased for compliance with a legal obligation
- restrict the processing of their data in specific circumstances,
- object to the processing of their data in specific circumstances,
- withdraw consent (where given),
- have personal data transmitted to another data controller and
- complain to the Information Commissioner.

Our policies

DCCC needs to collect and store personal data about its volunteers. Accordingly, we are committed to ensuring that our volunteers and Trustees comply with data protection law and maintain the security and integrity of personal data held by the charity in whatever form.

1. DCCC will not hold or process information about individuals without their knowledge and, where required, their consent.
2. DCCC will only hold information for specific purposes and will inform data subjects what those purposes are, how long we will store the data and their rights and we will also inform them if those change.
3. DCCC will never provide information to third parties unless necessary to comply with the law or other legitimate obligations (such as contracts of employment) or with the consent of the data subject. Should personal information be supplied to third parties in accordance with these policies, DCCC will comply with all the requirements of

GDPR including to ensure appropriate agreements are in place with such third parties.

4. Information will not be retained once it is not required for its stated purpose.
5. DCCC will seek to maintain accurate information whilst it is retained by creating ways in which data subjects can update the information held.
6. Data subjects will only receive communications from DCCC if they have consented to do so.
7. Data subjects are entitled to have access to information held about them by DCCC, subject to reasonable notice. Requests should be made in writing to Mrs Hilary Streak at: office@stpetersderby.org.uk
8. Data subjects are entitled to have data we hold about them corrected and/or completed.
9. Data subjects have the right to erasure of personal data we hold about them in circumstances set out in the GDPR.

DCCC has adopted procedures for ensuring the security of all personal data.

- Any DCCC Trustee or volunteer who has access to personal data will have received appropriate training over how it may be used.
- Paper records containing confidential personnel data are stored and disposed of in a secure way (i.e. in locked, non-portable secure storage containers).
- Electronic records are kept in a secure, encrypted, password protected environment that complies with GDPR requirements
- Data will not be transferred outside the EEA.

<u>Specific policies and procedures for DCCC volunteers</u>

Our responsibility to you:

Information about you	DCCC will keep a record of personal information about you, which may include details of your family, on our computer or manual files. Unless otherwise required by law, DCCC will treat such records as confidential and will only disclose relevant data to third parties where necessary to comply with the law and/or your contract of employment. The identity of such third parties and copies of the personal data can be made available to you by DCCC on request. We may provide relevant personal data regarding our volunteers to others on a strictly limited and confidential basis for the purposes of managing our charity, implementing our policies and procedures, health and safety purposes and other related matters.
How it's stored	We will ensure the security of all electronic and manual files at all times.
Access to information	You are entitled to make a request to see the information held about you at any time, in accordance with data protection law.

In order to do so, please put your request in writing to Mrs Hilary Streak at: office@stpetersderby.org.uk who will arrange to provide this information to you within 1 calendar month.

Information about others

Sometimes, giving access to personal data of the data subject cannot be done without revealing personal data about other individuals. Third party data should not normally be made available without the consent of the individuals concerned, although the law does not make this an absolute requirement. If we have the consent of those other individuals, then the information should be revealed. If we have not, then we will seek their consent if it is practicable.

If it is not practicable to seek consent, then we will have to consider whether, in the circumstances, the information can be revealed without it. Most cases are not likely to be simple, and we may have to seek specialist advice.

Your responsibility:

You are responsible for ensuring that:

- Any personal data that you hold, whether in electronic or paper format, is kept securely
- Personal information is not disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party
- Items that are marked 'personal' or 'private and confidential', or appear to be of a personal nature, are opened by the addressee only unless they have explicitly given permission for someone else to do so.

You should not use your office email address or DCCC email address for matters that are not work related.

In some situations, you may have access to personal data concerning individuals you are working with either internally or externally. Personal data is broadly defined as any information relating one or more identified or identifiable living person with information about them.

We have a responsibility to ensure that there is protection for any information through which an individual may be identified such as their:

- Name
- Address
- Telephone number
- Driving licence or passport number
- Date of birth
- Photograph

Or other information which, when combined with information about that

individual whose release could cause harm or distress, including:

- Bank/financial/credit card details
- National Insurance number
- Passport number/information on immigration status
- Tax, benefit or pension records
- Place of work
- Material related to social services (including child protection)
- Conviction/prison/court records/evidence
- Memberships of groups/affiliations/political.

How to treat personal information

In the first instance, please avoid printing anything containing personal information. If you do need to print this information, lock it away in your filing cabinets when you are not looking at it or using it, and shred it immediately you have finished with it.

Under no circumstances should you leave any documentation containing personal data unsecured in the office or take any documentation containing this sort of personal data out of the office.

If it is computerised, you must password protect documents or if kept on a USB, this must be password protected and kept securely in an encrypted environment.

Personal data should never be supplied to a third party without first receiving expert advice on the procedures to be followed when doing so.

When obtaining personal data from a data subject, you must in particular provide the data subject with the following further information to ensure fair and transparent processing:

- The period of time that the data will be stored.
- Their relevant rights under data protection law including right to rectification, erasure, restriction, objection and portability.
- The right to withdraw consent at any time.
- The right to lodge a complaint with the Information Commissioner.
- The consequences of the data subject's failure to provide data.

Personal data should not be obtained from any third party without first receiving expert advice on the procedures to be followed when doing so.

Data from business cards

We need to be particularly careful in our handling and use of business cards. Business cards cannot be automatically added to our mailing list without the individual's express consent. On receiving a business card ask the individual if they want to be on our mailing list and keep a record of that consent.

You must be careful about using DCCC's contact databases. All contacts held by DCCC must consent to being added to our marketing database. No sales or marketing contacts can be used for mass mailings containing individuals who have not opted-in. Of course, you are free to send individual emails to contacts in your database in the normal course of undertaking your job.

Failure to adhere to these guidelines can constitute an infringement of data protection law and make you and/or us liable to prosecution. It is essential that all DCCC volunteers are compliant with the law.

Mailing lists, databases and personal contact data

DCCC collects customer and stakeholder information and holds this in digital format for use as a mailing database. We must ensure we have processes that clearly delineate the management and collection of data in a marketing database for specific business purposes, in contrast to individual contact data held for individual use.