EDBF DUTY OF CARE: ORGANISATIONAL REPUTATION

DATA PROTECTION POLICY

Approver	Operations
Owner(s)	Manager – Operations
Classification	Culture
Original Issue Date	1 April 2016
Last Revision date	21 October 2019
Revised By	Manager – Operations
Next Revision Date	1 April 2021
Related Documents	• Data Protection
Location of Electronic Copy	• PeopleHR • 'H' Drive: 2019 Policies Folder
Scope	This Policy applies to all EDBF and EDPS Ltd employees plus those individuals identified in Paragraph 2. EDBF reserves the right to amend this policy at its discretion at any time. It does not form part of any employees' contract of employment with EDBF. Where EDBF is referred to in this policy, it is used as an umbrella term for both EDBF and EDPS Ltd.
Extensions	Individuals identified in Paragraph 2.
Exclusions	None

Data Protection Policy

Contents

1. Policy Statement

This policy sets out our rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

Everyone has rights with regard to how their personal information is handled. During the course of our activities we will collect, store and process personal information about our employees, and we recognise the need to treat it in an appropriate and lawful manner.

The types of information that we may be required to handle include details of current, past and prospective employees, suppliers, and others that we communicate with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in General Data Protection Regulation (GDPR) as it applies in the UK under the Data Protection Act 2018 (DPA 2018), The DPA 2018 gives clear guidance on how we may use such information.

If you consider that our provisions for complying with the Act have not been followed in respect of personal data about yourself or others you should raise the matter with your manager, the Operations Manager or one of the Data Protection Team.

In the event that this policy and the law conflict, the law shall take precedence. If employees are in any doubt as to what their rights are, they are to discuss matters with their manager. If this policy changes as a result of amendments in the law, the changes will be notified to the employee via their manager.

This policy does not form part of your contract of employment and it may be amended at any time.

2. Who is Covered by the Policy?

This policy is intended to apply to all employees of the Exeter Diocesan Board of Finance (hereafter referred to as EDBF) including full-time, part-time and fixed term employees and home workers. This policy also applies to all employees of EDPS Ltd.

In addition, it is intended that contractors, consultants, casual and agency staff and volunteers who undertake activities and duties authorised by EDBF or in a capacity viewed as officially representing EDBF also adhere to this policy. In such cases, the individuals will be made aware of this policy by their official supervisor along with our Electronic Information & Communications Systems Policy.

3. Definition of Data Protection Terms

Anonymisation: Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) by any means or by any person.

Consent: Any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her.

Contact: Any past, current or prospective parishioner, church member or member of the public.

Data: Covers information which is stored electronically, or in certain paper-based filing systems.

Data Controller: A natural or legal person, Public Authority, Agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

Data Processing: Any activity relating to the collection, recording, organising, structuring, use, amendment, storage, access, retrieval, transfer, analysis, disclosure, dissemination, combination, restriction, erasure or disposal of personal data.

Data Processing Agreement: Part of a contract of works to be carried out on behalf of a Data Controller, this sets out the terms under which personal data can be shared and processed by a Data Processor.

Data Processor: A natural or legal person, Public Authority, Agency or other body which Processes Personal Data on behalf of a Data Controller.

Data Protection: The process of safeguarding Personal Data from unauthorised or unlawful disclosure, access, alteration, Processing, transfer or destruction.

Data Protection Authority: An independent Public Authority responsible for monitoring the application of the relevant Data Protection regulation set forth in national law. The Information Commissioner's Office (ICO) is the recognised Data Protection Authority in the UK.

Data Subjects: For the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

Personal Data: Means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).

Data Controllers: Are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. We are the data controller of all personal data used in relation to the work undertaken by the Diocesan Board of Finance.

Data Users: Include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.

Data Processors: Include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on our behalf.

Identifiable Natural Person: Anyone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal Data: Any information which relates to an identified or Identifiable Natural Person.

Personal Data Breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

Process, Processed, Processing: Any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means. Operations performed may include collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling: Any form of automated processing of Personal Data where Personal Data is used to evaluate specific or general characteristics relating to an Identifiable Natural Person.

Pseudonymisation: Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) without a "key" that allows the data to be re-identified.

Special Categories of Data: (*also known as sensitive personal data*) Specific types of data that require additional care being taken when processing. The categories are: race, ethnic origin, politics, religion, trade-union membership; health; sex life; sexual orientation; genetic data; or biometric data (where used for ID purposes).

Subject Access Request: Data subjects' right to access their Personal Data.

Third Party: An external organisation with which EDBF conducts business and is also authorised to, under the direct authority of the Diocesan Secretary, process the personal data of diocesan contacts. They do not have the ability to make any decisions about how the data should be processed. They must always be designated through a contract or a Data Processing Agreement.

4. Data Protection Principles

The GDPR sets out the following principles related to the processing of personal data:

Principle 1: Lawfulness Fairness and Transparency

Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

This means that the Data Subject must be told who the data controller is, (in this case EDBF). They should be informed about the purpose for which data is to be processed (transparency). The Processing must match the description given to the Data Subject (fairness), and it must be for one of the purposes specified in the applicable Data Protection regulation (lawfulness).

Principle 2: Purpose Limitation

Personal Data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the GDPR and the DPA 2018. This means that personal data must not be collected for one purpose and then used for another.

Principle 3: Data Minimisation

Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

Principle 4: Accuracy

Personal Data shall be accurate and kept up to date.

Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed. Personal Data will only be kept for the period necessary to satisfy the permitted uses or applicable required retention period.

Principle 5: Storage Limitation

Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than the purposes for which the Personal Data is processed.

Personal data should not be kept longer than is necessary for the specified purpose. The length of time Personal Data may be retained is in accordance with the guidance

set out in the guide, “Save or Delete: the Care of Diocesan Records”, which is available from the Church of England website.

Care_of_diocesan_record_v2.1.pdf

Any Personal Data processed for the purposes of Safeguarding will be kept in accordance with our legal requirements and can be found in the guidance, ”Data Protection and Safeguarding in the Diocese of Exeter”, which is available from the

Diocese of Exeter website.
https://exeter.anglican.org/resources/safeguarding/resources/

Personal Data relating to clergy will be processed in accordance with the guidance set out in the House of Bishops’ guidance document, “Personal Files Relating to Clergy: Policy for Bishops and their staff”, which is available from the Church of England website.

Principle 6: Integrity and Confidentiality

Personal Data shall be 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.

Confidentiality means that only people who are authorised to use the data can access it.

Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.

This means that employees must use appropriate security measures to ensure the integrity and confidentiality of Personal Data is maintained at all times. This includes guarding against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

The Act requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor on the completion of a data sharing agreement which ensures that third-party processors agrees to comply with those procedures and policies, and have adequate measures in place.

Principle 7: Accountability

The Data Controller shall be responsible for, and be able to demonstrate, compliance.

This means that all employees must demonstrate that the Principles (outlined above) are met for all Personal Data for which they are responsible.

5. Processing in Line with Data Subject's Rights

Under the Data Protection legislation, data subjects have the following rights with regards to their personal information:

- The right to be informed about the collection and use of their personal data,
- The right to access personal data and supplementary information,
- The right to have inaccurate personal data rectified, or completed if it is incomplete,
- The right to erasure (to be forgotten) in certain circumstances,
- The right to data portability, which allows the data subject to obtain and reuse their personal data for their own purposes across different services,
- The right to object to processing in certain circumstances,
- Rights in relation to automated decision making and profiling,
- The right to withdraw consent at any time (where relevant),
- The right to complain to the Information Commissioner.

6. Data Security

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data. Employees should ensure that:

- In so far as possible, all Personal Data in your possession is kept secure from unauthorised access,
- Personal Data held on computer is protected with permissions managed to ensure access is restricted only to those who are entitled to access files,
- Paper files containing Personal Data are stored in locked cabinets, with access to keys limited to authorised employees,
- Personal Data that is transmitted to a third party electronically is only in encrypted form,
- Employees are vigilant, in particular when undertaking work off-site, and ensure that any Personal Data is not places in a position where it can be stolen or lost,
- All devices used to handle Personal Data are password protected and password are not shared with anyone,
- Personal Data is never stored on USB drives or other removable media unless encrypted and then only for the purpose of secure delivery,
- Secure delivery methods such as “guaranteed delivery” are used if sending Personal Data through the post,
- Electronic files are regularly backed up,

- Premises are properly protected with burglar and fire alarms,
- Desks are kept clear of Personal Data when employees are absent.

7. Methods of Disposal

Paper documents should be shredded. CD-ROMs should be physically destroyed when they are no longer required. All electronic media (CDs, DVDs, USB memory sticks, external hard drives, PDAs, mobile phones, etc.) should be returned to the Operations Manager for safe disposal when no longer required. Files should be deleted from the server when no longer required. E-mails should be deleted (& removed from 'Deleted Items') when no longer required. Electronic data should not be copied to other devices (including home computers) without authorisation from the IT Team. Please check with the IT Team if you are unsure of the implications of this when working through the Virtual Private Network (VPN), Outlook Web Access (OWA), exchange synchronisation, or any other method of accessing data or e-mails away from Diocesan IT equipment.

8. Equipment

Data users should ensure that individual monitors do not show confidential information to passers-by and that they lock their PC, phone etc. when they are left unattended. All laptops are provided with a cable to lock the laptop to your desk or other immovable object (if you do not have a cable or have lost a key, please speak to the IT Team).

9. Dealing with Subject Access Requests

Data Subjects have rights of access to their personal data which is held about them in both electronic and manual forms. Data subjects are entitled to obtain:

- Confirmation as to whether EDBF is processing any personal data about them.
- Access to their personal data.
- Any related information.

In order to exercise this right they must make a Data Subject Access Request (DSAR). The policy and application form for DSARs can be found here:

P:\Data Protection\Policies and Forms\DSAR policy and procedure v1 2.pdf

P:\Data Protection\Policies and Forms\DSAR App Form.docx

Employees who receive a DSAR should report it immediately to the DPT, by emailing dataprotection@exeter.anglican.org The DPT will log, oversee and track the progress of the request, and give guidance to employees about their responsibilities in relation to each request received.

10. Providing Information Over the Telephone

Any employee dealing with telephone enquiries should be careful about disclosing any personal information held by us. In particular they should:

- Never give out personal information over the telephone to external callers.
- In the event that the caller is persistent, employees can suggest that they take the caller's details and pass this onto the data subject to enable them to make contact with the caller.
- Refer to their manager or a member of the DPT for assistance in difficult situations. No-one should be bullied into disclosing personal information.

If you are asked to disclose Personal Data in an emergency and are uncertain about whether you should do so, check with your manager or the DPT to get the necessary authorisation. If you are unable to contact any of the above prior to disclosing the Personal Data, you must ensure that you inform your manager and the DPT as soon as reasonably practicable thereafter, in any event no later than 24 hours from the disclosure.

11. Complaints

If an individual is dissatisfied with the way that EDBF has dealt with an aspect of their data in relation to their rights under the GDPR and the DPA 2018, they should be advised to contact the Data Protection Team in the first instance:

dataprotection@exeter.anglican.org 01392 294901

If the data protection team are unable to satisfy the complaint, then individuals are advised to follow the complaints procedure, which can be found here:

https://exeter.anglican.org/wp-content/uploads/2017/10/Draft-EDBF-Complaints-Policy.pdf

If individuals are still dissatisfied, they can complain to the Information Commissioners Office, who can be contacted on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire. SK9 5AF.