THE CHURCH OF ENGLAND

DIOCESE OF SALISBURY

DATA PROTECTION POLICY

This policy applies to employees of the Diocesan Board of Finance (DBF) and volunteers undertaking work on behalf of the DBF

All employees are expected to comply with the provisions of the General Data Protection Regulation (GDPR).

GDPR – The Principles

Article 5 of the GDPR requires that personal data shall be:

a. Processed lawfully, fairly and in a transparent manner in relation to individuals;
b. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
c. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
f. 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, using appropriate technical or organisational measures.

Article 5(2) requires that:

> The controller shall be responsible for, and be able to demonstrate, compliance with the principles.

General Guidelines

All employees will be made aware of this policy and their duties under the GDPR.

The only people able to access personal data covered by this policy should be those who need it for their work.

Employees should keep all personal data secure by taking sensible precautions and following DBF guidelines.

Personal data should not be disclosed to unauthorised people either within the organisation or externally.

Personal data should be regularly reviewed. If found to be inaccurate it should be updated; if no longer required it should be deleted and disposed of.

Employees should request help from their line manager or the Data Protection Officer if they are unsure about any aspect of data protection.

Data Storage

Personal data kept on paper should be kept in a secure place where unauthorised people cannot access it.

Personal data stored electronically must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Personal data should be protected by strong passwords that are changed regularly and never shared between employees.
- Personal data should not be stored on removable media. If, however, personal data is temporarily loaded on removable media (eg memory stick, CD) for the purpose of a specific task, any changes should be transferred to the server and the personal data deleted from the removable media at the earliest opportunity (not exceeding seven days). All removable media containing personal data should be locked away securely when not being used. Files on removable media should be password protected.
- Personal data should only be stored on designated drives and servers in accordance with the Diocesan IT Policy.
- Personal data should not be stored on local drives, laptops or other mobile devices except in the case of authorised home workers with formally agreed data storage and protection processes in accordance with the Diocesan IT Policy.
- Personal data should be backed up frequently.
- All servers and computers containing data should be protected by approved security software and a firewall.

Data Use

When working with personal data, employees should ensure that computer screens are locked when left unattended.

Personal data should not be shared informally.

Personal data should be encrypted before being transferred electronically to authorised external contacts. Employees should ask the IT Manager for assistance if they need advice about this.

Personal data should never be transferred outside the European Economic Area.

Data Accuracy

In order to ensure that personal data is kept accurate and up to date employees should ensure that:

- It is held in as few places as necessary.
- It is reviewed regularly and updated promptly if found to be inaccurate or no longer required.
- It is updated as inaccuracies are discovered by informing the staff member(s) responsible for maintaining that data set.

Transparency

Individuals have a right to be given “fair processing information”. Employees should ensure that communications contain the relevant Privacy Notice to inform individuals:

- Who we are
- How we intend to use their data (information)
- The lawful basis for processing their data
- How long we keep it for

- How an individual can exercise their rights in respect of their data.

Privacy Notices can be found at (folder/file path).

Subject Access Requests

Individuals have the right to access their personal data so that they can check the lawfulness of the use and the accuracy of the data. The DBF must comply with any formal Subject Access Request within one month. The general principle is that as much information as possible should be shared with the individual. There are, however, limited categories of material that may be withheld in the interests of protecting the rights of other individuals to privacy, the prevention of crime, etc. Employees in receipt of such a request should refer in the first instance to the Data Protection Officer.

Data Protection By Design

The DBF recognises that "privacy by design" and data minimisation are now legal requirements. New projects and processes should consider any data protection implications from the outset in order to ensure legal compliance.

Data Breaches

The GDPR requires certain types of data breach to be formally notified to the Information Commissioner's Office (ICO) within 72 hours of the breach occurring. If an employee believes that a data breach has taken place they should inform the Data Protection Officer immediately. If the DPO is unavailable within the timeframe, advice should be sought from the Diocesan Registrar.

mjl
29.11.2017