THE CHURCH OF ENGLAND
DIOCESE OF NEWCASTLE

Data Protection Policy

1.0 Purpose of Policy

1.1 The Newcastle Diocesan Board of Finance (the Board) is committed to being transparent about how it collects and uses the personal data of its workforce, and to meeting its data protection obligations. This policy sets out the Board's commitment to data protection, and individual rights and obligations in relation to personal data.

1.2 The Diocesan Secretary is the person responsible for data protection compliance. The Secretary can be contacted at diosec@newcastle.anglican.org. Questions about this policy, or requests for further information, should be directed to the Secretary.

2.0 Scope of Policy

2.1 This policy applies to the personal data of job applicants, employees, contractors, volunteers, ecclesiastical office holders, apprentices and former employees, referred to as personal data.

2.2 It also applies to other personal data processed as part of the legitimate activities of the Diocese of Newcastle.

2.3 This policy, which is non-contractual, is issued by the Board and it may vary or amend the contents.

3.0 Definitions

3.1 **"Personal data"** is any information that relates to an individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

3.2 **"Special categories of personal data"** means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

3.3 **"Criminal records data"** means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

4.0 Underlying Data Protection Principles

4.1 The Board processes personal data in accordance with the following data protection principles:

- The Board processes personal data lawfully, fairly and in a transparent manner;
- The Board collects personal data only for specified, explicit and legitimate purposes;
- The Board processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing;

- The Board keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay;
- The Board keeps personal data only for the period necessary for processing;
- The Board adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

4.2 The Board tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons.

4.3 Where the Board processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with a policy on special categories of data and criminal records data.

4.4 The Board will update personal data promptly if an individual advises that his/her information has changed or is inaccurate.

4.5 Personal data gathered during the ecclesiastical appointment, employment, apprenticeship, contracting or volunteering relationship is held in the individual's record (in hard copy or electronic format, or both), and on electronic systems. The periods for which the Board holds personal data are contained in the Board's retention schedule.

4.6 The Board keeps a record of its processing activities in respect of personal data in accordance with the requirements of the UK General Data Protection Regulation (UK GDPR).

5.0 Individual Rights

5.1 As a data subject, individuals have a number of rights in relation to their personal data.

Subject access requests

Individuals have the right to make a subject access request. If an individual makes a subject access request, they are entitled to the following information:

- A description of the personal data;
- The purposes for which it is being processed;
- Recipients, retention period and rights of rectification, erasure, restriction and objections;
- Existence of automated decision making;
- Transfer safeguards.

5.2 The Board will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless he/she agrees otherwise.

5.3 To make a subject access request, the individual should send the request to info@newcastle.anglican.org or alternatively write to Church House, St John's Terrace, North Shields NE29 6HS. In some cases, the Board may need to ask for proof of identification before the request can be processed. The Board will inform the individual if it needs to verify his/her identity and the documents it requires.

5.4 The Board will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the Board processes large amounts of the individual's data, it may respond within three months of the date the request is received. The Board will write to the individual within one month of receiving the original request to tell him/her if this is the case.

5.5 If a subject access request is manifestly unfounded or excessive, the Board is not obliged to comply with it. Alternatively, the Board can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the Board has already responded. If an individual submits a request that is unfounded or excessive, the Board will notify him/her that this is the case and whether or not it will respond to it.

5.5 **Other rights**

Individuals have a number of other rights in relation to their personal data. They can require the Board to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override the Board's legitimate grounds for processing data (where the Board relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the Board's legitimate grounds for processing data.

5.6 To ask the Board to take any of these steps, the individual should send the request to info@newcastle.anglican.org or alternatively write to Newcastle Diocesan Board of Finance at Church House, St John's Terrace, North Shields NE29 6HS.

6.0 Data Security

6.1 The Board takes the security of personal data seriously. The Board has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees or office holders in the proper performance of their duties.

6.2 Personal data is stored with password protection and on electronic drives with restricted access. Physical copies are stored in locked filing cabinets and drawers. There is also restricted access to rooms beyond the public area.

6.3 Where the Board engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

7.0 Privacy Impact Assessments

7.1 Some of the processing that the Board carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, the Board will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

8.0 Data Breaches

8.1 If the Board discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. The Board will record all data breaches regardless of their effect.

8.2 If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

9.0 International Data Transfers

9.1 The Board will not transfer HR-related personal data to countries outside the United Kingdom.

10.0 Individual Responsibilities

10.1 Individuals are responsible for helping the Board keep their personal data up to date. Individuals should let the Board know if data provided to the Board changes, for example if an individual moves house or changes his/her bank details.

10.2 Individuals may have access to the personal data of other individuals in the course of their employment, contract, holding office, volunteer period or apprenticeship. Where this is the case, the Board relies on individuals to help meet its data protection obligations to other individuals.

10.3 Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the Board) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from the Board's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and

- not to store personal data on local drives or on personal devices that are used for work purposes.

Further details about the Board's security procedures can be found in its Information Security Policy.

10.4 Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the Board's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing personal data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

11.0 Training

11.1 The Board will provide training to all individuals about their data protection responsibilities as part of the induction process and when there are changes to legislation.

11.2 Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them

12.0 Roles and Responsibilities

11.1 Line manager responsibilities include:

- To familiarise themselves with the policy;
- To put in place measures to minimise the risk of data breaches;

Employee responsibilities include:

- To familiarise themselves with the Policy;
- To report to their manager as soon as possible if they believe there has been a data breach;

Human Resources responsibilities include:

- To provide advice and guidance to line managers and employees in respect of the Data Protection Policy.

13.0 Review

12.1 This policy will be reviewed every 2 years or as necessary if there is any change of legislation.