The Diocese of Northampton

DATA PROTECTION POLICY

Version 2.2 8th May 2018

Registered Charity No. 234091

CONTENTS

The Diocese of Northampton

DATA PROTECTION

DATA PROTECTION POLICY FOR THE DIOCESE OF NORTHAMPTON

1 INTRODUCTION AND BACKGROUND

1.1 The Diocese of Northampton (the "Diocese"), through its Trustees, is a Data Controller and consequently must process all Personal Data (including Special Categories of Personal Data) about Data Subjects in accordance with the General Data Protection Regulation 2016/679 (the "GDPR"), the Data Protection Act 2018, and any other relevant data protection legislation, domestic or otherwise, as may be in force or repealed or replaced from time to time (together, the "Data Protection Rules"). For the avoidance of doubt, the Diocese remains the sole Data Controller, even where Processing is carried out by its curial offices, parishes, departments and agencies. Please be aware that parishes form part of the Diocese and are not separate legal entities. Parishes are not Data Controllers nor do they process Personal Data on behalf of the Diocese as a Data Processor.

1.2 The Diocese will collect, store, use and otherwise process Personal Data about the people with whom it interacts, who are the Data Subjects. This may include parishioners, volunteers, clergy, employees, contractors, suppliers and other third parties.

1.3 The Diocese processes Personal Data so that it can comply with its statutory obligations and achieve its charitable objects of advancing and maintaining the Roman Catholic religion through the operation of its parishes and its other activities.

1.4 Every Data Subject has a number of rights in relation to how the Diocese processes their Personal Data. The Diocese is committed to ensuring that it processes Personal Data properly and securely in accordance with the Data Protection Rules, as such commitment constitutes good governance and is important for achieving and maintaining the trust and confidence of Data Subjects. Therefore, the Diocese will regularly review its procedures to ensure that they are adequate and up-to-date.

1.5 All clergy, staff and volunteers of the Diocese who are involved in the Processing of Personal Data held by the Diocese have a duty to protect the data that they process and must comply with this Policy. The Diocese will take any failure to comply with this Policy or the Data Protection Rules very seriously. Any such failure may result in legal action being taken against the Diocese or the individual responsible.

2 THE DATA PROTECTION PRINCIPLES

2.1 The Diocese as the Data Controller is required to comply with the six data protection principles set out in the GDPR, which provide that Personal Data must be:

2.1.1 Processed fairly, lawfully and in a transparent manner;

2.1.2 Collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with those purposes;

2.1.3 Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

2.1.4 Accurate and, where necessary, kept up to date – every reasonable step must be taken to ensure

that inaccurate personal data is erased or rectified without delay;

2.1.5 Kept in a form that permits identification of Data Subjects for no longer than is necessary for the purposes for which the personal data is processed; and

2.1.6 Processed in a way that ensures its security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational security measures.

2.2 There is also an overarching principle; the Data Controller must be able to demonstrate compliance with the six principles. Accountability is vital.

3 THE DIOCESAN DATA PROTECTION MANAGER AND REGISTRATION WITH THE ICO

3.1 The Diocesan Trustees have overall responsibility for compliance with the Data Protection Rules. However, the diocesan Data Protection Manager (the "DPM") shall be responsible for ensuring day-to-day compliance with this Policy and with the Data Protection Rules. The DPM will undergo training at least once every 12 months and the Diocese will provide the DPM with sufficient resources and support to carry out their responsibilities. The DPM's name and contact details can be found in section 10 of this Policy.

3.2 The DPM will liaise with the Heads of Diocesan departments and agencies, or their nominees, regarding Data Protection Rules compliancy and implementation of this Policy within their offices; and with Parish Priests or their nominees, for the same purposes within parishes.

3.3 The Diocese is registered with the Information Commissioner's Office (the "ICO") as a Data Controller and will remain so at least until the end of 24 May 2018, as is required by law. The Diocese will be responsible for paying to the ICO any future fees levied on Data Controllers by the Data Protection Rules.

3.4 This Policy applies to all Personal Data processed by the Diocese in whatever format (e.g. paper, electronic, film) and regardless of how it is stored (e.g. electronically or in filing cabinets). It also includes information that is in paper form but is intended to be put into electronic form, and to any recordings made, such as telephone recordings and CCTV.

4 HOW THE DIOCESE WILL COMPLY AND DEMONSTRATE COMPLIANCE

4.1 This Policy is intended to ensure that any Processing of Personal Data is in accordance with the Data Protection Rules and the Data Protection principles. The Diocese will therefore:

4.1.1 Ensure that, when personal information is collected (whether direct from the individual or from a third party), the Data Subject is provided with, or informed how to inspect, a Privacy Notice and informed of what data is being collected and for what legitimate purpose(s);

4.1.2 Be transparent and fair in processing Personal Data;

4.1.3 Take steps to ensure the accuracy of data at the point of collection and at regular intervals thereafter, including advising Data Subjects of their right to ask for rectification of Personal Data held about them;

4.1.4 Securely dispose of inaccurate or out-of-date data, or data which is no longer required for the purpose(s) for which it was collected;

4.1.5 Share information with others only when it is lawful to do so and ensure that individuals are informed of the categories of recipient to whom data will or may be disclosed and the purposes of any such disclosures;

4.1.6 Ensure that additional safeguards (as required by the Data Protection Rules) are in place to protect Personal Data that is transferred outside of the European Economic Area (the "EEA") (see section 7.4 of

this Policy);

4.1.7 Ensure that data is processed in line with the Data Subject's rights, which include the right to:

(a) Request access to Personal Data held about them by the Diocese (including, in some cases, having it provided to them in a commonly used and machine-readable format);

(b) Have inaccurate Personal Data rectified;

(c) Have the processing of their Personal Data restricted in certain circumstances;

(d) Have Personal Data erased in certain specified situations (in essence where the continued processing of it does not comply with the Data Protection Rules);

(e) Prevent the processing of Personal Data for direct-marketing purposes (which includes for fundraising and wealth screening purposes

(f) Ask the Diocese to prevent Processing of Personal Data which is likely to cause unwarranted or substantial damage or distress to the Data Subject or any other individual; and

4.1.8 Ensure that all clergy, volunteers and employees are aware of and understand the Diocese's Data Protection policies and procedures; and

4.1.9 Adopt a Data Retention Schedule which sets out the periods for which different categories of Personal Data will be kept.

4.2 Through adherence to this Policy and related Data Protection policies, and through appropriate record-keeping, the Diocese will seek to demonstrate compliance with each of the Data Protection principles.

4.3 In addition, the Data Protection Rules require the Data Controller to carry out a Data Protection Impact Assessment (a "DPIA") prior to undertaking any Processing of Personal Data that is "likely to result in a high risk for the rights and freedoms" of individuals. DPIAs will therefore be considered where appropriate in relation to the implementation of any new projects, services or systems which could result in a high privacy risk to individuals (particularly where new technology is being deployed). Please contact the DPM for guidance (see section 10 of this Policy).

5 DATA SECURITY & RESPONSIBILITIES OF CLERGY, STAFF AND VOLUNTEERS

5.1 The Diocese must ensure that appropriate technical and organisational security measures are in place to prevent unauthorised or unlawful Processing or damage to or loss (accidental or otherwise), theft, or unauthorised disclosure of Personal Data (a "Data Breach"). In particular, all clergy, employees and volunteers should ensure that:

5.1.1 The only individuals who have access to Personal Data and are able to process it are those who are authorised to do so;

5.1.2 Personal Data is stored only on central Diocesan computer systems at its various offices, and on parish-owned computers, or on secure Cloud-based services, and not on individually-owned PCs, portable electronic devices or removable storage media, unless those devices and their use are compliant with the BYOD Policy;

5.1.3 Passwords are kept confidential, are changed periodically and are not shared between individuals;

5.1.4 PCs are locked or logged off and paper documents are securely locked away when individuals are away from their desks for substantial periods;

5.1.5 Offices, desks and filing cabinets/cupboards are kept locked if they contain Personal Data of any

kind, whether in digital or electronic format or on paper;

5.1.6 When destroying Personal Data, paper documents are securely shredded and electronic data is securely deleted; and

5.1.7 Personal Data removed from an office is subject to appropriate security measures, including keeping paper files in a place where they are not visible or accessible by the public; using passwords/passcodes; encrypting portable electronic devices and storing such devices securely (e.g. not left in the boot of a car overnight, or visible in a car when temporarily parked).

Further detail on the Diocese's requirements in relation to IT security are set out in the IT Security Policy.

5.2 In the event that you become aware that there has been a Data Breach, you must report this immediately to the DPM, following the Data Breach Procedure, at brin@nrcdfinance.com. Further contact details for the DPM can be found in section 10 of this Policy.

6 PROCESSING ; LAWFUL GROUNDS

The Diocese processes personal data on a number of lawful grounds or bases, including:

Lawful Ground for Processing of Personal Data	***Examples***
Where we have an individual's consent	*Posting photographs of an individual on a diocesan website* *Providing information for the administration of a wedding* *Sending individuals marketing or fundraising communication by email or text*
Where it is necessary for the performance of a contract to which an individual is party	*An employment contract ; or, where an individual enters into a hiring agreement for one of our facilities*
Where it is necessary for compliance with a legal obligation	*Passing on information to a local authority, HM Revenue & Customs, or the Charity Commission*
Where it is necessary to protect the vital interests of an individual	*Passing on information to the Police* *Passing on information about an individual's serious health condition to the NHS or a health professional where there is a risk of death or serious injury to that person or another individual*
Where it is necessary for performance of a task in the public interest	*Updating and maintaining the civil register of marriages* *Carrying out safeguarding activities*
Where is it necessary for the purposes of the legitimate interests pursued by the Diocese or a third party	*This will cover most of what the Diocese and its parishes do. A specific example would be - Using baptism data to follow up with families for First Communion*

The Data Protection Rules require further conditions for processing “Special Category” personal data, which includes data “revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, . . . genetic data and biometric data [processed] for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation”.

It is likely that at least some of the Diocese’s data processing will come under this heading as revealing the religious beliefs of the data subjects.

Further Conditions for Processing of Special Categories of Data	***Examples***
Where we have an individual's explicit consent	*To cater for an individual's dietary or medical needs at an event* *To supply sacramental information about them, at their request, to a parish elsewhere*
Where it is necessary for compliance with a legal obligation	*Passing on information to the local authority or HMRC*
Where it is necessary to protect the vital interests of an individual	*Passing on information to the Police* *Passing on information about an individual's serious health condition to the NHS or a health professional where there is a risk of death or serious injury to that person or another individual*
Where it is carried out in the course of the Diocese's legitimate activities as a not-for-profit body with religious aims, and the data relates only to members of the Diocese and is not disclosed outside the Diocese	*Using parishioners' health related data for pastoral visits* *Carrying out a parish census* *Parish rotas and group lists*
Where information has manifestly been made public	*Where an individual has made their Catholic beliefs clear in public media, or the data already appears in a publically-available source such as a Directory*
Where we are establishing, exercising or defending legal claims	*Providing information to our insurers or lawyers in connection with legal proceedings*
Where the processing is for reasons of substantial public interest	*Where steps are taken to prevent fraud or other dishonest activity*
Where the processing is necessary for archiving historical records	*Maintenance of Diocesan archives and parish records*

Lawful Ground for Processing of Criminal Convictions & Offences Data	**Examples**
Where the Diocese is exercising obligations or rights which are imposed or conferred by law on it or the data subject in connection with employment, social security or social protection and the Diocese has an appropriate policy document in place	*To undertake appropriate checks on individuals prior to taking up a role*
Where it is necessary for the prevention or detection of an unlawful act	*Passing on information to the Police or other investigatory body*
Where the Diocese is complying with or assisting others to comply with regulatory requirements relating to unlawful acts or dishonesty	*Passing on information to the Police or other investigatory body*
Where it is carried out in the course of safeguarding children or other individuals at risk	*Making a safeguarding disclosure*
Where information is disclosed for insurance purposes	*Ensuring the Diocese has appropriate insurance cover*
Where an individual has given their consent to the	

processing	
Where the Diocese is establishing, exercising or defending legal claims	*Providing information to our insurers or lawyers in connection with legal proceedings*
Where it is necessary to protect the vital interests of an individual	*Passing on information to the Police*
Where it is carried out in the course of the Diocese's legitimate activities by a not-for-profit body with religious aims	*Carrying out pastoral activities*

7.1 **DISCLOSING AND SHARING PERSONAL DATA**

7.1.1 When receiving telephone or email enquiries, clergy, employees and volunteers should exercise caution before disclosing any Personal Data. The following steps should be followed:

(a) Ensure the identity of the person making the enquiry is verified and check whether they are entitled to receive the requested information;

(b) Require the enquirer to put their request in writing so that their identity and entitlement to receive the information can be verified if the information is particularly sensitive and/or you are not confident the person is entitled to the information;

(c) If there is any doubt, refer the request to the DPM for assistance (particularly where Special Categories of Personal Data are involved); and

(d) When providing information, ensure that Personal Data is securely packaged and sent by the most appropriate means (e.g. special delivery, courier or hand delivery) in accordance with the Data Protection Rules, the Privacy Notice and this Policy. Personal data should not be sent in, or attached to, insecure e-mails.

7.1.2 Please remember that parents and guardians are only entitled to access information about their child if the child is unable to act on their own behalf (e.g. because the child is not mature enough to understand their rights) or if the child has given their consent. If you are unsure about whether or not to provide information about a child to a parent or guardian, please speak to the DPM before providing any information. Children from 12 years upwards are generally to be taken as being capable of understanding their rights and making decision regarding their own information. However, consideration of the particular circumstances and the child's capacity must be given in each circumstance.

7.1.3 Please also remember that individuals are only entitled to obtain information about themselves and not any other third parties (e.g. a family member, other parishioner or member of clergy or staff).

7.2 **DATA PROCESSORS**

7.2.1 The Diocese may instruct another body or organisation to process Personal Data on its behalf as a Data Processor (e.g. a payroll provider, or a third party IT provider). In such situations, the Diocese will share necessary information with the Data Processor, but will remain responsible for compliance with the Data Protection Rules as the Data Controller.

7.2.2 Personal Data will only be transferred to a third-party Data Processor if the DPM is satisfied that the third party has in place adequate policies and procedures to ensure compliance with the Data Protection Rules. There should also be a written contract in place between the Diocese and the Data Processor, which includes provisions to ensure that the Data Processor complies with the requirements of the Data

Protection Rules. If you have authority to enter into such contracts, please refer to the Data Processor Contract Checklist.

7.3 THIRD PARTY REQUESTS

7.3.1 The Diocese may from time to time receive requests from third parties for access to documents containing Personal Data. The Diocese may disclose such documents to any third party where it is legally required or permitted to do so. Such third parties may include health professionals, the Police and other law enforcement agencies, the Charity Commission, HMRC, other regulators, immigration authorities, insurers, local authorities (e.g. Trading Standards), Courts and Tribunals or organisations seeking references.

7.3.2 Anyone in receipt of any verbal or written request from any person for access to, or disclosure of, any Personal Data outside of normal Diocesan operations must immediately contact the DPM.

7.4 TRANSFERS OF PERSONAL DATA OUTSIDE OF THE EEA

7.4.1 The Data Protection Rules require Data Controllers to put additional safeguards in place when transferring Personal Data outside of the EEA (e.g. to the Vatican). Additionally, such transfers can only take place on a number of legal grounds. The Diocese does not store Personal Data outside of the UK. Where it contracts with a Data Processor who holds data on behalf of the Diocese outside the EEA, very strict compliancy will be sought.

However, the Diocese may transfer Personal Data outside of the EEA where requested by the Data Subject, on the basis of the Data Subject's informed consent. This includes, but is not limited to, the situation where a Data Subject requires their marriage record to be sent to a non-EEA country. The DPO may also authorise transfers where another legal ground in the Data Protection Rules is met.

7.5 SUBJECT ACCESS REQUESTS (SAR'S)

7.5.1 Any Data Subject may exercise their rights as set out above (e.g. the right of access to the Personal Data which the Diocese holds about them, or the right to have Personal Data erased). Any and all such requests should immediately be referred to the DPM.

7.5.2 To be valid, a Subject Access Request must be made in writing (including requests made via email or on social media) and provide enough information to enable the Diocese to identify the Data Subject and to comply with the request.

7.5.3 All Subject Access Requests will be dealt with by the DPM. Clergy, employees or volunteers who receive a Subject Access Request must forward it to the DPM immediately in order that such requests can be replied to within the strict deadlines set out in the Data Protection Rules (generally one month from the date of the request).

7.5.4 No fees will be charged for dealing with Subject Access Requests unless a request is considered to be manifestly unfounded, excessive or repetitive. Fees may be charged to provide additional copies of information previously provided. Where the Diocese considers a request to be manifestly unfounded, excessive or repetitive, the Diocese may lawfully refuse to respond and, if so, the DPM will inform the Data Subject of this in writing within the one-month period.

8 FUNDRAISING AND MARKETING

8.1 Any use of Personal Data for marketing (including fundraising) purposes must comply with the Data Protection Rules and the Privacy and Electronic Communications Regulations (the "PECR") (and any replacement legislation), which relate to marketing by electronic means.

8.2 Individuals have a right to object to their Personal Data being used for electronic marketing purposes. Individuals must be informed of their right to object when their data is collected. If an objection is received, no further marketing or fundraising communications must be sent to them.

8.3 The PECR requires that the Diocese has the prior consent of recipients in certain circumstances before it sends any unsolicited electronic messages for the purpose of fundraising, or other marketing activities (e.g. events).

9 MONITORING AND REVIEW

9.1 This policy will be reviewed every 12 months and may be subject to change.

10 CONTACTS

10.1 Any queries regarding this Policy should be addressed to the Diocesan Data Protection Manager, Brin Dunsire, who can be contacted by email at brin@nrcdfinance.com, by telephone on 01844 273337 or 01604 712065, or at the following address:

The Data Protection Manager, Bishops House, Marriott Street, Northampton NN2 6AW.

10.2 Complaints will be dealt with in accordance with standard Diocesan procedures

10.3 Further advice and information can be obtained from the Information Commissioner's Office at www.ico.org.uk

11 OTHER INFORMATION-GOVERNANCE POLICIES

11.1 This Policy must be read in conjunction with:

11.1.1 Privacy Notice

11.1.2 Data Retention Schedule

11.1.3 IT Security Policy and Bring-Your-Own-Device Policy

12 GLOSSARY

"Data Controller" means a person, organisation or body that determines the purposes for which, and the manner in which, any Personal Data is processed. A Data Controller is responsible for complying with the Data Protection Rules and establishing practices and policies in line with them.

"Data Processor" means any person, organisation or body that Processes personal data on behalf of and on the instruction of the Diocese. Data Processors have a duty to protect the information they process by following the Data Protection Rules.

"Data Subject" means a living individual about whom the Diocese processes Personal Data and who can be identified from the 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 and the information that the Diocese holds about them.

"EEA" is the European Economic Area, consisting of the countries of Austria, Belgium, Bulgaria, Czech Republic, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, **Iceland**, Ireland, Italy,

Latvia, **Liechtenstein**, Lithuania, Luxembourg, Malta, Netherlands, **Norway**, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, United Kingdom. (Countries in bold are non-EU members. Switzerland is in neither, nor is the Vatican City.)

"Personal Data" means any information relating to a living individual who can be identified from that information or in conjunction with other information which is in, or is likely to come into, the Diocese's possession. Personal Data can be factual (such as a name, address or date of birth) or it can be an opinion (e.g. a performance appraisal). It can even include a simple email address. A mere mention of someone's name in a document does not necessarily constitute Personal Data, but personal details such as someone's contact details or salary (if it enabled an individual to be identified) would fall within the definition.

"Processing" means any activity that involves use of Personal Data. It includes obtaining, recording or holding the information or carrying out any operation or set of operations on it, including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring or disclosing Personal Data to third parties.

"Special Categories of Personal Data" (previously called sensitive personal data) means information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexuality. It also includes genetic and biometric data. Special Categories of Personal Data can only be processed under strict conditions and such processing will usually, although not always, require the explicit consent of the Data Subject.

"Data Breach" - A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data. It can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

This policy was approved by the Diocesan Trustees on: 20th April 2018

The next review is due on or before: 1st May 2019

v. 2.2 8 May 2018 BD