ARCHDIOCESE OF ST ANDREWS & EDINBURGH

DATA PROTECTION POLICY

FOREWORD

Edinburgh, the Solemnity of the Most Sacred Heart of Jesus, 2018

To the clergy and faithful of the Archdiocese of St Andrews & Edinburgh

The Church is the guardian of the truth that Jesus Christ is risen from the dead. Since the first Pentecost she has been obedient to her divine Master's command and ceaselessly carried this Good News to every place and culture (cf. Mt 28:19). In the early years of mission, St Peter counselled the first Christians that, wherever they found themselves, they were to be model citizens and respectful of authority and those who made the law (cf. 1Pt 2:17).

The Church in Scotland finds herself the subject of the two jurisdictions of Scots and Canon Law. Recently changes in the law of the land with regard to how we store and use the private information of third parties have come into force. In order to facilitate the observance of these new civil laws in this Archdiocese and best practice, the following regulations *Data Protection in the Archdiocese of St Andrews & Edinburgh* are to be adopted. This will be a valuable *vademecum* for our clergy and those who assist in the administration of the Curia and our parishes.

I would therefore ask you to help put it into effect and, in the coming years, reflect upon its effectiveness and assist in it perfection, for the sake of the common good and in order to be compliant with both our canonical and civil responsibilities.

With my thanks to those who have helped to assemble this policy and to our clergy and people who will be implementing it across the Archdiocese, I am

Yours sincerely in Christ,

✠Leo Cushley
Archbishop of St Andrews & Edinburgh

DATA PROTECTION POLICY FOR THE ARCHDIOCESE OF ST ANDREWS & EDINBURGH

1 INTRODUCTION AND BACKGROUND

1.1 The Archdiocese of St Andrews & Edinburgh (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(the "**GDPR**") and any other relevant data protection legislation, domestic or otherwise, (as may be in force or repealed or replaced from time to time) (the GDPR). 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, not less than once a year.

1.5 All Trustees, 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, and to demonstrate compliance, 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 OFFICER 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 Officer (the "**DPO**")] shall be responsible for ensuring day-to-day compliance with this Policy and with the Data Protection Rules. The DPO will undergo training at least once every 12 months and the Diocese will provide the DPO with sufficient resources and support to carry out their responsibilities. The DPO's name and contact details can be found in paragraph 11 of this Policy.

3.2 The Diocesan Trustees and the DPO will be assisted in fulfilling their Data Protection Policy compliance responsibilities by Curial Managers, Parish Priests, other clergy, other employees and parishioners who volunteer.

4 Parish Priests

The Parish Priests have overall responsibility for ensuring our compliance with Data Protection legislation within their Parish.

They will ensure that:

- the Diocesan Data Protection Policy is implemented and communicated effectively
- a data protection culture of continuous improvement is created and progress monitored
- suitable and sufficient funds, people, materials and equipment are provided to meet all data protection requirements
- parish Data Protection Representatives are appointed to provide data protection assistance
- there is regular communication and consultation with employees and volunteers on data protection issues
- employees and Parish Safety and Safeguarding Representatives are encouraged to attend Diocesan data protection training programmes
- Diocesan systems of work and risk assessment procedures provided by the Diocesan DPO are implemented
- Data protection incidents are recorded, investigated and reported to the Diocesan DPO

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 February 2020 as is required by law.

4.1 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.

5 HOW THE DIOCESE WILL COMPLY AND DEMONSTRATE COMPLIANCE

5.1 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:

5.1.1 ensure that, when personal information is collected (whether direct from the individual or from a third party), the Data Subject is provided with a Privacy Notice and informed of what data is being collected and for what legitimate purpose(s); In the case of children <12 years old registering for their sacraments, their parent / guardian will be provided with a Privacy Notice.

5.1.2 be transparent and fair in processing Personal Data;

5.1.3 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;

5.1.4 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;

5.1.5 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;

5.1.6 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 8.3 of this Policy);

5.1.7 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

(g) prevent, in some cases, decisions being made about them which are based solely on automated processing (i.e. without human intervention) and which produce significant or legal effects on them;

5.1.8 ensure that all clergy, volunteers and employees are aware of the Diocese's data protection policies and procedures and their own responsibilities in terms of data protection, and understand that failure to comply may result in disciplinary sanctions in the event of non-adherence or breach; and

5.1.9 adopt, monitor and keep under review, a data retention schedule which sets out the periods for which different categories of Personal Data will be kept. To follow

5.2 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.

5.3 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) and will consider other regulation relevant to data protection, such as the Privacy and Electronic Communications Regulations. Please contact the DPO for guidance (see paragraph 11 of this Policy).

6 DATA SECURITY & RESPONSIBILITIES OF CLERGY, STAFF AND VOLUNTEERS

6.1 The Diocese shall 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:

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

6.1.2 personal Data is stored only on the central Diocesan computer system and not on individual PCs, portable electronic devices or removable storage media, unless those devices are compliant with the BYOD Policy OR are subject to appropriate measures of password protection, encryption and remote deletion;

6.1.3 passwords are kept confidential, are changed regularly and are not shared between individuals;

6.1.4 PCs are locked or logged off and paper documents are securely locked away when individuals are away from their desks;

6.1.5 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;

6.1.6 when destroying Personal Data, paper documents are securely shredded and electronic data is securely deleted; and

6.1.7 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).

[Further detail on the Diocese's requirements in relation to IT security are to follow]

6.2 In the event that you become aware that there has been a Data Breach, you must report this immediately to the Data Protection Officer following the Data Breach Procedure at chancellor@staned.org.uk. Further contact details for the DPO can be found in paragraph 11 of this Policy.

7 PRIVACY NOTICE

7.1 When any Personal Data is collected from an individual, they must be provided with a Privacy Notice. The Privacy Notice provides information about what, why and how information is processed. You should make yourself aware of it.

8 PROCESSING, DISCLOSURE AND SHARING OF INFORMATION

The Diocese processes personal data for a number of different purposes, including:

Lawful Ground for Processing of Personal Data	**Examples**
Where we have an individual's consent Or that of their parent / guardian (in case of children <12 (or 16?) years old)	Posting photographs of an individual on a diocesan website Providing information for the administration of a sacrament (e.g. Baptism, Confirmation, Wedding)
Where it is necessary for the performance of a contract to which an individual is party	Providing information to a photographer about photos required for a wedding
Where it is necessary for compliance with a legal obligation	Passing on information to the local authority
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 register of marriages (plus baptism?) Carrying out safeguarding activities
Where is it necessary for the purposes of the legitimate interests pursued by the Diocese or a third party	Using baptism data to follow up with families for first communion Using funeral data to invite relatives of the deceased to memorial Masses.

Lawful Ground 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
Where it is necessary for compliance with a legal obligation	Passing on information to the local authority
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 by a not-for-profit body with religious aims	Using parishioners' health related data for pastoral visits Providing information to other Catholic Dioceses if you move home or are being provided services by a marriage tribunal
Where information has manifestly been made public	Referring to a public figure who is well known as a member of the church, as a Catholic
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 we are arranging insurance for a group pf parishioners in advance of a pilgrimage
Where the processing is necessary for maintenance of records required by Canon Law	Maintenance of 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

8.1 **DISCLOSING PERSONAL DATA**

8.1.1 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;

(c) 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.

(d) No Personal Data must be disclosed to any enquirer save and except in accordance with this policy and any statutory obligations of the Diocese; and

(e) if there is any doubt, refer the request to the Data Protection Officer for assistance (particularly where Special Categories of Personal Data are involved)

8.1.2 Please remember that parents and guardians are only entitled to access information about their child (by making a request) 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 Data Protection Officer before providing any information.

Data Processors

8.1.3 The Diocese may instruct another body or organisation to process Personal Data on its behalf as a Data Processor (e.g. a payroll provider, 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.

8.1.4 Personal Data will only be transferred to a third party Data Processor if the Data Protection Officer 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.

8.2 THIRD PARTY REQUESTS

8.2.1 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.

8.2.2 Normal not-for-profit body with religious aims requests, for example another diocese or religious body seeking confirmation that their marriage candidate is free to do so and has been baptised and/or confirmed.

8.2.3 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 Data Protection Officer.

8.3 TRANSFERS OF PERSONAL DATA OUTSIDE OF THE EUROPEAN ECONOMIC AREA ("EEA")

8.3.1 The Data Protection Rules require Data Controllers to put additional safeguards in place when transferring Personal Data outside of the EEA. Additionally, such transfers can only take place on a number of legal grounds. 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 baptismal, Confirmation or marriage record to be sent to a non-EEA country. Transfers may also take place where another legal ground in the Data Protection Rules is met.

8.4 **SUBJECT ACCESS REQUESTS (SARS)**

8.4.1 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).

8.4.2 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. This includes requests made via email or on social media.

8.4.3 All Subject Access Requests will be dealt with by the Data Protection Officer. Clergy, employees or volunteers who receive a Subject Access Request must forward it to the Data Protection Officer 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).

8.4.4 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 Data Protection Officer will inform the Data Subject of this in writing within the one-month period.

9 FUNDRAISING AND MARKETING

9.1 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.

9.2 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. 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).

Any use of Personal Data for fundraising or direct marketing purposes which is not in accordance with the requirements set out above must be approved, in advance, by the DPO.

10 MONITORING AND REVIEW

10.1 This policy will be reviewed at least every 12 months, in accordance with the Trustees' programme of policy review, and may be subject to change.

11 CONTACTS

11.1 Any queries regarding this Policy should be addressed to the Diocesan Data Protection Officer, The Reverend Scott T Deeley, The Chancellor, Archdiocese of St Andrews & Edinburgh, 100 Strathearn Road, Edinburgh, EH9 1BB or email chancellor@staned.org.uk or telephone 0131 623 8900. Contact details can also be found on the diocesan website www.archdiocese-edinburgh.com

Complaints will be dealt with in accordance with the diocesan Complaints Policy. Further advice and information can be obtained from the Information Commissioner's Office at www.ico.org.uk

12 OTHER INFORMATION GOVERNANCE POLICIES

12.1 This Policy must be read in conjunction with the attached:

12.1.1 Privacy Notice

12.1.2 Data Protection Policy

12.1.3 Data Retention Policy - *to follow*

12.2 Forms attached:

12.2.1 Gift Aid Single Donation form with Privacy Policy

12.2.2 Gift Aid Multiple Donation form with Privacy Policy

12.2.3 Keeping in Touch with Us – Parish Form

13 GLOSSARY OF TERMS

"Diocese" means the Archdiocese of St Andrews & Edinburgh.

"**Data Controller**" has a specific meaning within the General Data Protection Regulation. It means a person, organisation or body that determines the purposes for which, and the manner in which, any Personal Data is processed. Across its curial offices, parishes, departments and agencies, the Diocese is the sole Data Controller, even where Processing is carried out by those curial offices, parishes, departments and agencies. The Diocese, as

Data Controller, has a responsibility to comply with the Data Protection Rules and establish 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 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.

"**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.