**St Francis Xavier Foreign Mission Society Trust**

**known as Xaverian Missionaries**

**General Data Protection Policy**

**Data Controller**

St Francis Xavier Foreign Mission Society Trust, a Trust registered in Scotland No. SC012905 with centres across the UK at Xaverian Missionaries’ Centre, Calder House, Calder Avenue, Coatbridge, ML5 4JS; Xaverian Missionaries’ Centre 169 Sharoe Green Lane, Fulwood, Preston PR2 8HE and the Parish of St. Bartholomew’s in Glasgow.

**Data Protection Officer**

Ian Bathgate, located at the Coatbridge address above and contactable on 01236 606364 or by email at dpoibathgate@gmail.com.

# **Introduction**

The Xaverian Missionaries are a religious based missionary congregation who here in the UK undertake services to the Parish entrusted to them by the Archdiocese of Glasgow (at Present St. Bartholomew’s – Castlemilk) and are involved in activities and events whose aim is both the economic support of an identified project in one of the countries in which the congregation is present as well as raising the awareness of the local church, communities and individuals with whom we come in contact about situations in other parts of our world. As a result, the Xaverian Missionaries need to gather and use certain information (personal and sensitive data) about individuals. These individuals can include specific persons, organisations, employees that the trust has a relationship with or may need to contact. This policy describes how this personal data must be collected, handled and stored to meet the trust’s data protection standards and to comply with the law.

# **Why this policy exists**

This data protection policy ensures Xaverian Missionaries:

* complies with data protection law and follows good practice
* protects the rights of staff, contacts and individuals within related entities
* is open about how it stores and processes individuals’ personal and sensitive data
* protects itself from the risks of a data breach

# **Data protection law**

Data Protection Law describes how we must collect, handle and store personal and sensitive data. These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with data protection law, personal data must be collected and used fairly, stored safely and must not be disclosed unlawfully.

Data Protection Law is underpinned by the following important principles. These principles state that personal data must 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 is 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; and

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.

## **Policy scope**

This policy applies to all personal and sensitive data that the trust holds relating to identifiable individuals, even if that information technically falls outside of existing Data Protection Law. This can include:

* names of individuals;
* postal addresses;
* email addresses;
* telephone numbers; and
* any other information that is relating to individuals

## **Data protection risks**

This policy helps to protect Xaverian Missionaries from some very real data security risks, including:

* breaches of confidentiality. For instance, information being given out inappropriately;
* failing to offer choice. For instance, all individuals should be free to choose how the trust uses data relating to them; and
* reputational damage. For instance, the trust could suffer damage should hackers successfully gain access to personal and sensitive data.

## **Responsibilities**

The Xaverian Missionaries take ultimate responsibility for data protection.

Everyone who works for or with Xaverian Missionaries also has some responsibility for ensuring data is collected, stored and is handled and processed in line with this policy and the data protection principles, as contained within Data Protection legislation.

If you have concerns or wish to exercise any of your rights under the GDPR or other UK Data Protection Law, then you can contact the data protection officer, Ian Bathgate at dpoibathgate@gmail.com.

# **Process and Procedures**

# The Xaverian Missionaries will:

* ensure that the legal basis for processing personal data is identified in advance and that all processing complies with the law;
* not do anything with personal, sensitive data (including special category data), that you would not expect given the content of this policy and the trust’s privacy notice;
* ensure that appropriate privacy notices are in place advising staff and others how and why their data is being processed, and, in particular, advising data subjects of their rights;
* only collect and process the personal data that it needs for purposes it has identified in advance;
* ensure that, as far as possible, the personal data it holds is accurate, or a system is in place for ensuring that it is kept up to date as far as possible;
* only hold onto your personal data for as long as it is needed, after which time the Xaverian Missionaries will securely erase or delete the personal data. See the section below on data retention periods;
* ensure that appropriate security measures are in place to ensure that personal data can only be accessed by those who need to access it and that it is held and transferred securely.

The Xaverian Missionaries will ensure that all staff who handle data on its behalf are aware of their responsibilities under this policy and other relevant data protection and information security policies, and that they are adequately trained and supervised.

Breaching this policy may result in disciplinary action for misconduct, including dismissal. Obtaining (including accessing) or disclosing personal data in breach of Xaverian Missionaries’ data protection policies may also be a criminal offence.

**For how long does the trust keep data?**

The trust will hold personal data for as long as necessary. Consideration shall therefore be given to determine the appropriate retention period in order to ensure that personal data is retained for as long as the trust is legally required to retain such data and there being no other legal basis for retaining such data beyond this period. The trust shall ensure that personal and sensitive data is confidentially destroyed or if in electronic format deleted from our computer network.

# **Data storage**

These rules describe how and where data should be safely stored. When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see or access it.

These guidelines also apply to data that in printed format:

* When not required, the paper or files should be kept in a locked drawer or filing cabinet.
* Employees shall make sure paper and printouts are not left where unauthorised people could see them.
* Printed documents which contain confidential, personal or sensitive data shall not be left on desks, printers or left accessible overnight.
* Data printouts shall be shredded and disposed of securely when no longer required.

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

* Data should be protected by strong passwords that are changed regularly and never shared between employees.
* If data is stored on removable media (like a CD or DVD or Memory stick), these should be kept locked away securely when not being used.
* Data should only be stored on designated drives and servers and should only be uploaded to an approved software solution.
* Where possible, servers containing personal data should be sited in a secure location, away from general office space.
* Data should be backed up frequently. These backups should be tested regularly, in line with the trust’s standard backup procedures.
* Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
* All servers and computers containing data should be protected by approved security software and a firewall.

# **Data use**

Personal data is of no value to the Xaverian Missionaries unless we can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

* Personal data should not be shared informally. In particular, it should never be sent in the body of an email or as an attachment to an email, as this form of communication is not secure.
* Personal data must be encrypted before being transferred electronically.
* Personal data should never be transferred outside of the European Union.
* Employees should not save copies of personal data to their own computers.

# **Data accuracy**

Data Protection law requires the Xaverian Missionaries to take reasonable steps to ensure data is kept accurate and up to date. The more important it is that the personal data is accurate, the greater the effort the Xaverian Missionaries should put into ensuring its accuracy.

It is the responsibility of the trust and all employees who work with personal data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

* Data will be held in as few places as necessary.
* Every opportunity should be taken to ensure data is updated. For instance, by confirming a caller’s details when they call.
* The Xaverian Missionaries will make it easy for data subjects to update the information it holds about them.
* Data should be updated as inaccuracies are discovered. For instance, if an individual or contact can no longer be reached on their stored telephone number, it should be removed from the database or record held.

# **Data Subject Rights**

The Xaverian Missionaries has processes in place to ensure that it can facilitate any request made by an individual to exercise their rights under data protection law.

Subject Access

All individuals who are the subject of personal data held by the Xaverian Missionaries are entitled to request information about how personal data is being processed, including whether personal data is being processed and the right to be allowed access to that data and to be provided with a copy of that data along with the right to obtain the following information:

* the purpose of the processing;
* the categories of personal data;
* the recipients to whom data has been disclosed or which will be disclosed;
* the retention period;
* the right to lodge a complaint with the Information Commissioner’s Office;
* the source of the information if not collected direct from the subject; and
* the existence of any automated decision making.

If an individual should contact the trust requesting this information, this is called a subject access request. Subject access requests from individuals should be made by email, addressed to the Data Protection Officer at dpoibathgate@gmail.com.

The Xaverian Missionaries will facilitate any request from a data subject who wishes to exercise their rights under data protection law as appropriate, always communicating in a concise, transparent, intelligible and easily accessible form and without undue delay.

The trust will aim to provide the relevant data in response to a subject access request within 1 month. Note for more complicated requests this may take up to two months. The trust will always verify the identity of anyone making a subject access request before handing over any information.

Rectification

Data subjects have the right to request that personal data is rectified if it is found to be inaccurate or incomplete.

Erasure

Data subjects have the right to have data erased and to have confirmation of erasure, but only where:

* the data is no longer necessary in relation to the purpose for which it was collected; or
* where consent is withdrawn; or
* where there is no legal basis for the processing; or
* there is a legal obligation to delete data.

Restriction of processing

Data subjects have the right to ask for certain processing to be restricted in the following circumstances:

* if the accuracy of the personal data is being contested; or
* if our processing is unlawful but the data subject does not want it erased; or
* if the data is no longer needed for the purpose of the processing but it is required by the data subject for the establishment, exercise or defence of legal claims; or
* if the data subject has objected to the processing, pending verification of that objection.

Data Portability

Data subjects have the right to receive a copy of personal data which has been provided by the data subject and which is processed by automated means in a format which will allow the individual to transfer the data to another data controller. This would only apply if the Xaverian Missionaries was processing the data using consent or on the basis of a contract.

Object to processing

Data subjects have the right to object to the processing of personal data relying on the legitimate interests processing condition within the data protection legislation unless the Xaverian Missionaries can demonstrate compelling legitimate grounds for the processing which override the interests of the data subject.

**Data Breaches**

If you discover that there has been a breach of personal or sensitive data (including special category data) that may pose a risk to the rights and freedoms of individuals, you must report this in the first instance to the trust’s data protection officer. The trust shall then follow procedures to investigate and where appropriate ensure that the Information Commissioner’s Office is notified of the breach within 72 hours of becoming aware of the breach. It is therefore important that all breaches are notified at the earliest opportunity. Failure to notify a breach within these timescales could involve a fine being imposed on the trust.

The trust will record all data breaches regardless of their effect or degree of risk, however only those breaches relevant to the category above shall be reportable to the Information Commissioner’s Office. The trust shall therefore maintain a Data Breach Register and shall identify and implement the appropriate corrective actions as appropriate.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will inform the affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken. The importance of notifying the trust of a breach is therefore highly significant and a requirement under the current Data Protection Law.

**Monitoring and review**

This policy was last updated on 25 May 2018 and shall be regularly monitored and reviewed, at least every two years, or as and when Data Protection Law is amended.