The Indian Orthodox Church CLG (St. Thomas Indian Orthodox Church)

Malankara House, Old Lucan Road, Palmerstown, Dublin 20, D20 VP97, Ireland.

Charity Reg. No - 17764

DATA PROTECTION POLICY

Adopted: [Date]

Contents

1. About our Church

The Malankara Orthodox Syrian Church, refers to the section of the St. Thomas Christians of India, that Canonically came under Catholicate of the East whose Supreme Head is His Holiness

The Indian Orthodox Church company limited by guarantee (CLG) is a Parish of the Malankara Orthodox Syrian Church (hereinafter referred to as "Parish/Our Parish"). We are a fully registered charitable organization registered with the Company Registrar and the Charity Commissioners. Our other registered names are St. Thomas Charitable Foundation and St. Thomas Indian Orthodox Church. we carry on the business of a Christian church engaged in the advancement of Christianity, to further diocesan activities, to support the clergy and to support the upkeep of the church and to organizes church services and prayer meetings.

Our Parish is committed to protecting all information that we handle about people we support and work with, and to respecting people's rights around how their information is handled. This policy explains our responsibilities and how we will meet them.

Section B – What this policy is for

2. Policy statement

1.1 Our Parish is committed to protecting personal data and respecting the rights of our **data subjects**; the people whose **personal data** we collect and use. We value the personal information entrusted to us and we respect that trust, by complying with all relevant laws and adopting good practice.

We process personal data to help us:

a) provide pastoral support for members and others connected with our church;

b) provide services to our community

c) maintain our list of church members and regular attendees;

d) provide general updates, news, create parish publications, Christmas/birthday or similar wishes, events, annual reports, charity/donation request, activities and spiritual notifications

e) safeguard children, young people, and adults at risk;

f) recruit, support and manage staff and volunteers;

g) undertake research

h) promote the spiritual interest of the congregation

i) maintain our accounts and records;

j) maintain the security of property and premises;

k) claiming Charity donations refund from Revenue Commissioner

l) To share your contact details with the Church Regional, Diocesan and Catholicate office

a) respond effectively to enquirers and handle any complaints [and]

b) provide eligibility list for AGM / EGM participation and electoral list

2.2 This policy has been approved and adopted by the parish management committee and the board of directors who are responsible for ensuring that we comply with all our legal obligations. It sets out the legal rules that apply whenever we obtain, stores or uses personal data.

3. Why this policy is important

3.1 We are committed to protecting personal data from being misused, getting into the wrong hands as a result of poor security or being shared carelessly, or being inaccurate, as we are aware that people can be upset or harmed if any of these things happen.

3.2 This policy sets out the measures we are committed to taking as an organization and, what each of us will do to ensure we comply with the relevant legislation.

3.3 In particular, we will make sure that all personal data is:

a) processed **lawfully, fairly and in a transparent manner**;

b) processed for **specified, explicit and legitimate purposes** and not in a manner that is incompatible with those purposes;

c) **adequate, relevant and limited to what is necessary** for the purposes for which it is being processed;

d) **accurate** and, where necessary, up to date;

e) **not kept longer than necessary** for the purposes for which it is being processed;

f) processed in a **secure** manner, by using appropriate technical and organisational means;

g) processed in keeping with the **rights of data subjects** regarding their personal data.

4. Policy scope

4.1 This policy applies to us and all staff, post-holders, volunteers, members, contractors, suppliers and other people processing personal data on behalf of us.

4.2 It applies to all data that we hold relating to identifiable individuals. This can include for example:

a) Names of individuals, postal/email addresses, date of birth, baptism date, date of marriage and telephone numbers.

b) Sensitive personal data such as information in relation to physical or mental health conditions, religious beliefs, ethnic origin, sexual orientation.

5. Underlying Principles

5.1 The law is complex, but there are a number of underlying principles, including that personal data:

c) will be processed lawfully, fairly and transparently.

d) is only used for a specific processing purpose that the data subject has been made aware of and no other, without further consent.

e) collected on a data subject should be “adequate, relevant and limited.” i.e. only the minimum amount of data should be kept for specific processing.

f) must be “accurate and where necessary kept up to date”

g) should not be stored for longer than is necessary, and that storage is safe

6. How this policy applies to you & what you need to know

As an employee, vicar, trustee, secretary, board members, committee members, any members and volunteers processing personal information on behalf of the church, you are required to comply with this policy. If you think that you have accidentally breached the policy it is important that you contact our Data Protection Lead immediately so that we can take swift action to try and limit the impact of the breach.

Anyone who breaches the Data Protection Policy may be subject to disciplinary action, and where that individual has breached the policy intentionally, recklessly, or for the personal benefit they may also be liable to prosecution or to regulatory action.

6.1 **[As a leader/assigned member/committee member:** You are required to make sure that any procedures that involve personal data, that you are responsible for in your area, follow the rules set out in this Data Protection Policy.]

6.2 **As a data subject of our parish**: We will handle your personal information in line with this policy.

6.3 **As an appointed data processor/contractor:** Companies who are appointed by us as a data processor are required to comply with this policy under the contract with us. Any breach of the policy will be taken seriously and could lead to us taking contract enforcement action against the company, or terminating the contract. Data processors have direct obligations under the GDPR, primarily to only process data on instructions from the controller (us) and to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk involved.

6.4 **Our Data Protection Lead is** responsible for advising Our Parish and its staff and members about their legal obligations under data protection law, monitoring compliance with data protection law, dealing with data security breaches and with the development of this policy. Any questions about this policy or any concerns that the policy has not been followed should be referred to them at **office@indianorthodoxireland.ie**

6.5 Before you collect or handle any personal data as part of your work (paid or otherwise) for Our Parish, it is important that you take the time to read this policy carefully and understand what is required of you, as well as the organisation's responsibilities when we process data.

6.6 Our procedures will be in line with the requirements of this policy, but if you are unsure about whether anything you plan to do, or are currently doing, might breach this policy you must first speak to the Data Protection Lead.

7. Training and guidance

7.1 We will provide general training at least annually for all staff to raise awareness of their obligations and our responsibilities, as well as to outline the law.

7.2 We may also issue procedures, guidance or instructions from time to time. [Managers/leaders/committee members must set aside time for their team to look together at the implications of their work.]

Section B – Our data protection responsibilities

8. What personal information do we process?

8.1 In the course of our work, we may collect and process information (personal data) about many different people (data subjects). This includes data we receive straight from the person it is about, for example, where they complete forms or contact us. We may also receive information about data subjects from other sources including, for example, previous employers [and other examples].

8.2 We process personal data in both electronic and paper form and all this data is protected under data protection law. The personal data we process can include information such as names and contact details, education or employment details, [other examples] and visual images of people.

8.3 In some cases, we hold types of information that are called **"special categories"** of data in the GDPR. This personal data can only be processed under strict conditions.

> **'Special categories' of data** (as referred to in the GDPR) includes information about a person's: racial or ethnic origin; political opinions; religious or similar (e.g. philosophical) beliefs; trade union membership; health (including physical and mental health, and the provision of health care services); genetic data; biometric data; sexual life and sexual orientation.

8.4 We will not hold information relating to criminal proceedings or offences or allegations of offences unless there is a clear lawful basis to process this data such as where it fulfils one of the substantial public interest conditions in relation to the safeguarding of children and of individuals at risk or one of the additional conditions relating to criminal convictions set out in either Part 2 or Part 3 of Schedule 1 of the Data Protection Act 2018.

8.5 Other data may also be considered 'sensitive' such as bank details but will not be subject to the same legal protection as the types of data listed above.

9. Making sure processing is fair and lawful

9.1 Processing of personal data will only be fair and lawful when the purpose for the processing meets a legal basis, as listed below, and when the processing is transparent. This means we will provide people with an explanation of how and why we process their personal data at the point we collect data from them, as well as when we collect data about them from other sources.

9.2 Legitimate **interest** (routine church management & updates via social media, lists of group members with very minimal personal data involved etc.).

9.3 Vital Interest e.g. using emergency contact details

9.4 Contract (e.g. processing visa requirements for Priest, letting out the church building or hall, Lease or renting Churches/premises),

How can we legally use personal data?

9.5 Processing of personal data is only lawful if at least one of these legal conditions, as listed in Article 6 of the GDPR, is met:

a) the processing is **necessary for a contract** with the data subject;

b) the processing is **necessary for us to comply with a legal obligation**;

c) the processing is necessary to protect someone's life (this is called "**vital interests**");

d) the processing is **necessary for legitimate interests** pursued by our parish or another organisation unless these are overridden by the interests, rights and freedoms of the data subject.

e) If none of the other legal conditions applies, the processing will only be lawful if the data subject has given their clear **consent**.

How can we legally use 'special categories' of data?

9.6 Processing of 'special categories' of personal data is only lawful when, in addition to the conditions above, one of the extra conditions, as listed in Article 9 of the GDPR, is met. These conditions include where:

a) the processing is necessary for **carrying out our obligations under employment and social security and social protection law**;

b) the processing is necessary for **safeguarding the vital interests** (in emergency, life or death situations) **of an individual** and the data subject is incapable of giving consent;

c) the processing is carried out in the **course of our legitimate activities** and only relates to our members or persons we are in regular contact with in connection with our purposes;

d) the processing is necessary for **pursuing legal claims**.

e) If none of the other legal conditions applies, the processing will only be lawful if the data subject has given their **explicit consent**.

9.7 Before deciding which condition should be relied upon, we may refer to the original text of the GDPR as well as any relevant guidance, and seek legal advice as required.

What must we tell individuals before we use their data?

9.8 If personal data is collected directly from the individual, we will inform them [in writing] about; our identity/contact details [and those of the Data Protection Lead, the reasons for processing, and the legal bases, [including explaining any automated decision making or profiling], explaining our legitimate interests, and explaining, where relevant, the consequences of not providing data needed for a contract or statutory requirement; who we will share the data with; if we plan to send the data outside of the European Union; how long the data will be stored and the data subjects' rights.

This information is commonly referred to as a 'Privacy Notice'.

This information will be given at the time when the personal data is collected.

9.9 If data is collected from another source, rather than directly from the data subject, we will provide the data subject with the information described in section 9.8 as well as: the categories of the data concerned; and the source of the data.

This information will be provided to the individual in writing and no later than within 1 month after we receive the data unless a legal exemption under the GDPR applies. If we use the data to communicate with the data subject, we will at the latest give them this information at the time of the first communication.

If we plan to pass the data onto someone else outside of Our Parish apart from Diocesan information that we need to provide, we will give the data subject this information before we pass on the data.

10. When we need consent to process data

10.1 Where none of the other legal conditions applies to the processing, and we are required to get consent from the data subject, we will clearly set out what we are asking consent for, including why we are collecting the data and how we plan to use it. Consent will be specific to each process we are requesting consent for and we will only ask for consent when the data subject has a real choice whether or not to provide us with their data.

10.2 Consent can, however, be withdrawn at any time and if withdrawn, the processing will stop. Data subjects will be informed of their right to withdraw consent and it will be as easy to withdraw consent as it is to give consent.

11. Processing for specified purposes

11.1 We will only process personal data for the specific purposes explained in our privacy notices (as described above) or for other purposes specifically permitted by law. We will explain those other purposes to data subjects in the way described above, unless there are lawful reasons for not doing so.

12. Data will be adequate, relevant and not excessive

12.1 We will only collect and use personal data that is needed for the specific purposes described above (which will normally be explained to the data subjects in privacy notices). We will not collect more than is needed to achieve those purposes. We will not collect any personal data "just in case" we want to process it later.

13. Accurate data

13.1 We will make sure that personal data held is accurate and, where appropriate, kept up to date. The accuracy of personal data will be checked at the point of collection and at appropriate points later on.

14. Keeping data and destroying it

14.1 We will not keep personal data longer than is necessary for the purposes that it was collected for. We will comply with official guidance issued to our sector about retention periods for specific records.

14.2 Information about how long we will keep records for can be found in our Data Retention Schedule.

14.3 The violation of the constitution of Malankara Orthodox Church, 1934 and regulations of the Parish can lead to termination of your rights to be a member of this Parish. Any grievance redress shall be supervised by the Parish Vicar and Committee, in consultation with the Diocesan Bishop.

15. Security of personal data

15.1 We will use appropriate measures to keep personal data secure at all points of the processing. Keeping data secure includes protecting it from unauthorised or unlawful processing, or from accidental loss, destruction or damage.

15.2 We will implement security measures which provide a level of security which is appropriate to the risks involved in the processing.

Measures will include technical and organisational security measures. In assessing what measures are the most appropriate we will take into account the following, and anything else that is relevant:

a) the quality of the security measure;

b) the costs of implementation;

c) the nature, scope, context and purpose of processing;

d) the risk (of varying likelihood and severity) to the rights and freedoms of data subjects;

e) the risk which could result from a data breach.

15.3 Measures may include:

a) technical systems security;

b) measures to restrict or minimise access to data;

c) measures to ensure our systems and data remain available or can be easily restored in the case of an incident;

d) physical security of information and of our premises;

e) organisational measures, including policies, procedures, training and audits;

f) regular testing and evaluating of the effectiveness of security measures.

16. Keeping records of our data processing

16.1 To show how we comply with the law we will keep clear records of our processing activities and of the decisions we make concerning personal data (setting out our reasons for those decisions).

Section C – Working with people we process data about (data subjects)

17. Data subjects' rights

17.1 We will process personal data in line with data subjects' rights, including their right to:

a) request access to any of their personal data held by us (known as a Subject Access Request);

b) ask to have inaccurate personal data changed;

c) restrict processing, in certain circumstances;

d) object to processing, in certain circumstances, including preventing the use of their data for direct marketing;

e) data portability, which means to receive their data, or some of their data, in a format that can be easily used by another person (including the data subject themselves) or organisation;

f) not be subject to automated decisions, in certain circumstances; and

g) withdraw consent when we are relying on consent to process their data.

17.2 If a colleague receives any request from a data subject that relates or could relate to their data protection rights, this will be forwarded to our Data Protection Lead immediately.

17.3 Parish members as responsible citizens are requested to restrain from any sought of unauthorized video/audio recordings/Mobile phone or social media depiction of worship or any other Parish proceedings. Any violations of privacy according to data protection laws of the state against any individual/or Parish by any member is strictly barred under rights of privacy. All such violations depicting or demeaning in electronic or print media shall be denounced by the Parish and considered as grievous to the integrity of the member. These violations shall be dealt with in accordance with the GDPR policy.

17.4 We will act on all valid requests as soon as possible, and at the latest within one calendar month, unless we have reason to, and can lawfully extend the timescale. This can be extended by up to two months in some circumstances.

17.5 All data subjects' rights are provided free of charge.

17.6 Any information provided to data subjects will be concise and transparent, using clear and plain language.

18. Direct marketing

18.1 We will comply with the rules set out in the GDPR, the Privacy and Electronic Communications Regulations (PECR) and any laws which may amend or replace the regulations around **direct marketing**. This includes, but is not limited to, when we make contact with data subjects by post, email, text message, social media messaging, telephone (both live and recorded calls) and fax.

> **Direct marketing** means the communication (by any means) of any advertising or marketing material which is directed, or addressed, to individuals. "Marketing" does not need to be selling anything or be advertising a commercial product. It includes contact made by organisations to individuals for the purposes of promoting the organisation's aims.

18.2 Any direct marketing material that we send will identify Our Parish as the sender and will describe how people can object to receiving similar communications in the future. If a data subject exercises their right to object to direct marketing we will stop the direct marketing as soon as possible.

Section D – working with other organisations & transferring data

19. Sharing information with other organisations

19.1 We will only share personal data with other organisations or people when we have a legal basis to do so and if we have informed the data subject about the possibility of the data being shared (in a privacy notice) unless legal exemptions apply to inform data subjects about the sharing. Only authorised and properly instructed members are allowed to share personal data.

19.2 We will keep records of information shared with a third party, which will include recording any exemptions which have been applied, and why they have been applied. We will follow

the DPC's statutory ***Data Sharing Code of Practice*** (or any replacement code of practice) when sharing personal data with other data controllers. Legal advice will be sought as required.

20. Data processors

20.1 [Before appointing a contractor who will process personal data on our behalf (a data processor) we will carry out due diligence checks. The checks are to make sure the processor will use appropriate technical and organisational measures to ensure the processing will comply with data protection law, including keeping the data secure and upholding the rights of data subjects. We will only appoint data processors who can provide us with sufficient guarantees that they will do this.]

20.2 [We will only appoint data processors on the basis of a written contract that will require the processor to comply with all relevant legal requirements. We will continue to monitor the data processing, and compliance with the contract, throughout the duration of the contract.]

21. Transferring personal data outside the European Union (EU)

21.1 Personal data cannot be transferred (or stored) outside of the European Union unless this is permitted by the GDPR. This includes storage on a "cloud" based service where the servers are located outside the EU.

21.2 We will only transfer data outside the EU where it is permitted by one of the conditions for non-EU transfers in the GDPR

Section E – Managing change & risks

22. Data protection impact assessments

22.1 When we are planning to carry out any data processing which is likely to result in a high risk we will carry out a Data Protection Impact Assessment (DPIA). These include situations when we process data relating to vulnerable people, trawling of data from public profiles, using new technology, and transferring data outside the EU. Any decision not to conduct a DPIA will be recorded.

22.2 We may also conduct a DPIA in other cases when we consider it appropriate to do so. If we are unable to mitigate the identified risks such that a high risk remains we will consult with the DPC.

22.3 DPIAs will be conducted in accordance with the DPC's Code of Practice 'Conducting privacy impact assessments'.

23. Dealing with data protection breaches

23.1 To exercise all relevant rights, queries or complaints please in the first instance contact Data Protection Lead at **office@indianorthodoxireland.ie**

23.2 Where staff or volunteers, [or contractors working for us], think that this policy has not been followed, or data might have been breached or lost, this will be reported **immediately** to the Data Protection Lead.

23.3 We will keep records of personal data breaches, even if we do not report them to the DPC.

23.4 We will report all data breaches which are likely to result in a risk to any person, to the DPC. Reports will be made to the DPC within **72 hours** from when someone in the church becomes aware of the breach.

23.5 In situations where a personal data breach causes a high risk to any person, we will (as well as reporting the breach to the DPC), inform data subjects whose information is affected, without undue delay.

This can include situations where, for example, bank account details are lost or an email containing sensitive information is sent to the wrong recipient. Informing data subjects can enable them to take steps to protect themselves and/or to exercise their rights.

Section E – Internet and Electronic Communication

Our Vicar and office appointed members are permitted to access assigned office emails. Email and social media Passwords are changed frequently. It is the responsibility of the individual to maintain the integrity of such usage by adapting to data protection rules. IT administrator should be consulted for any clarifications for usage information or handover information.

It is a must that passwords should be changed during position handover. Passwords should not be shared or recycled. Data Protection Lead should be immediately informed in the event of such data breach related with Passwords.

Creation of new/continuing/on behalf/unlisted church-related social sharing media such as Websites/Twitter/WhatsApp/Google or similar media for sharing data should be allowed only after approved by Data protection Lead who may take the internal necessary approval from the Church Committee.

All Church Personnel, regardless of the role they play in ministering to the faithful, are bound by the following:

Overview

- It is not acceptable for Church Member to engage in the repeated, persistent monitoring and/or patrolling of online activity of the young people to whom they minister without a legitimate reason.

- Church Member should never consider electronic communication (emails, social networking sites, text message, etc.) to be private and should not be used to address/discuss confidential matters.

- Church Member should address and model online safety with minors when used as part of their program

Email

- Use the official provided email account on a device that is protected by anti-virus software.
- Do not communicate with minors to whom you minister using your personal email address.
- Do not share a minor's email address with others without prior permission of parents or guardians.
- Report any violation of this policy to our Data Protection Lead

Online Video and Chat

- Parent/guardian permission is required for Parish-related online video and/or chat sessions between Church Personnel and minors.
- Church Personnel must obtain permission from an appropriate legitimate authority to initiate and/or engage in Parish-related online video and/or chat sessions with members and minors
- Only authorised members who are in the role of Trustee or Secretary or Vicar can send SMS on behalf of our Parish with the consent of Data Protection Lead

Text Messaging

- Because one-on-one text messaging between Church Personnel and minors is not appropriate when using Mobile Text Data (Texting) and Short Messaging Service (SMS), Church Personnel must adhere to the following:
- Church Personnel should not respond to inappropriate or personal text messages from minors to whom they minister and are required to inform the appropriate legitimate authority.
- Only authorised members who are in the role of Trustee or Secretary or Vicar can send SMS on behalf of our Parish.

Blogs and Microblogs

- Blogs used for educational or Parish purposes must be approved by the Church Committee and the content should reflect the purpose. Access by the Data Protection Lead or IT web administrator is a condition of approval.
- The owner of the blog must be diligent in monitoring for inappropriate activity.
- Personal blogs should not be intentionally shared with minors or Parish use.

Social Media Ministry Use

- Data Protection Lead or IT Administrator must give permission for Church Personnel to establish a social networking site related to the parish, Sunday school or any approved spiritual organization.

Technology in Ministry:

- Permission to post from the social media account must be granted by the Data Protection Lead

- A social media account should only be used as a virtual billboard to post details of school or parish events, and must not be used as a means of one-on-one communication. Digital relationships which link to other accounts must be specifically related to ministry purposes.

- Images or videos of minors or events may only be posted on a ministry online account if those in the images or videos grant specific permission. Church Personnel must comply with requests from a parent that images or videos be removed.

- Non-public personal information must not be posted.

Private Use

- Volunteers, who are not otherwise defined as Church Personnel, may not communicate with minors via social media without written permission of a parent or guardian.

- Church Personnel who use social networking sites to communicate with minors about their ministry must use an account registered in the name of the parish or diocese.

Direct Messaging Any services that include the ability for direct messaging are subject to all of the rules stated herein.

Photographs and Audio, Video Recording

- Devices capable of capturing, transmitting, or storing images or recordings may never be accessed or operated in restrooms, dressing rooms, sleeping areas, or other areas where there is a reasonable expectation of privacy.

- Audio and/or video recordings are not permitted without the expressed consent of those being recorded.

24. Review

This policy and related data protection procedures will be reviewed on an annual basis by the Data Protection Lead to reflect best practice in data management, security and control and to ensure compliance with GDPR.

Signed:

Position:

Date:

Review Date:

Schedule 1 – Definitions and useful terms

The following terms are used throughout this policy and have their legal meaning as set out within the GDPR. The GDPR definitions are further explained below:

Data controller means any person, company, authority or other body who (or which) determines the means for processing personal data and the purposes for which it is processed. It does not matter if the decisions are made alone or jointly with others.

The data controller is responsible for the personal data which is processed and the way in which it is processed. We are the data controller of data which we process.

Data processors include any individuals or organisations, which process personal data on our behalf and on our instructions e.g. an external organisation which provides secure waste disposal for us. This definition will include the data processors' own staff (note that staff of data processors may also be data subjects).

Data subjects include all living individuals who we hold or otherwise process personal data about. A data subject does not need to be an Irish national or resident. All data subjects have legal rights in relation to their personal information. Data subjects that we are likely to hold personal data about include:

a) Members, the people we care for and support;
b) our employees (and former employees);
c) consultants/individuals who are our contractors or employees working for them;
d) volunteers;
e) tenants;
f) trustees;
g) complainants;
h) supporters;
i) enquirers;
j) friends and family;
k) advisers and representatives of other organisations.

DPC means the Information Commissioners Office which is Ireland's regulatory body responsible for ensuring that we comply with our legal data protection duties. The DPC produces guidance on how to implement data protection law and can take regulatory action where a breach occurs.

Personal data means any information relating to a natural person (living person) who is either identified or is identifiable. A natural person must be an individual and cannot be a company or a public body. Representatives of companies or public bodies would, however, be natural persons.

Personal data is limited to information about living individuals and does not cover deceased people.

Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

Privacy notice means the information given to data subjects which explains how we process their data and for what purposes.

Processing is very widely defined and includes any activity that involves the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing can also include transferring personal data to third parties, listening to a recorded message (e.g. on voicemail) or viewing personal data on a screen or in a paper document which forms part of a structured filing system. Viewing of clear, moving or stills images of living individuals is also a processing activity.

Special categories of data (as identified in the GDPR) includes information about a person's:

l) Racial or ethnic origin;

m) Political opinions;

n) Religious or similar (e.g. philosophical) beliefs;

o) Trade union membership;

p) Health (including physical and mental health, and the provision of health care services);

q) Genetic data;

r) Biometric data;

s) Sexual life and sexual orientation.

Pseudonymisation
Pseudonymisation takes the most identifying fields within a database and replaces them with artificial identifiers, or pseudonyms. For example a name is replaced with a unique number. The purpose is to render the data record less identifying and therefore reduce concerns with data sharing and data retention

Encryption
Encryption is a mathematical function using a secret value — the key — which encodes data so that only users with access to that key can read the information. In many cases encryption can provide an appropriate safeguard against the unauthorised or unlawful processing of personal data, especially in cases where it is not possible to implement alternative measures.

Data Controller: Our Parish

Charity Reg. No - 17764

Address:

Malankara House, Old Lucan Road, Palmerstown, Dublin 20, D20 VP97, Ireland.
Charity Reg. No - 17764

References

http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html

https://www.dataprotection.ie/docs/appointing-a-Data-Protection-Officer/1717.htm

Revision History

Version Number	Date	Author/Owner	Description of Change
1.0	15/07/2018	Binoy Abraham	Baseline version
2.0	27/07/2018	Binoy Abraham	Charity name, name clarifications and logo is updated.
3.0	27/07/2018	Binoy Abraham	Draft Version consolidated for Church Management committee review and updated changes