PERSONAL DATA PROTECTION POLICY OF [TRUE JESUS CHURCH (SINGAPORE)]

1. INTRODUCTION

1.1 **True Jesus Church (Telok Kurau)** respects the right of individuals to protect their personal data. The Church is committed to protecting the privacy of every individual's personal data in accordance with its obligations under the Personal Data Protection Act 2012 ("**PDPA**").

1.2 To comply with our obligations under the PDPA, we have produced this Personal Data Protection Policy ("**Policy**"). This Policy sets out what we must do when any personal data of an individual is collected, used or disclosed and it also seeks to provide general guidance as to how to collect, handle, store or transmit personal data that we may receive in the course of administering the affairs of the Church.

1.3 This Policy applies to all personnel of the Church, which includes all Pastoral Staff and Office Staff, whether employed or voluntary, and all Ministry leaders. All personnel of the Church must familiarize themselves and comply with the obligations, policies and practices set out in this Policy.

1.4 Compliance with the PDPA is important, because a failure to observe the obligations under the PDPA could potentially expose the Church, the Pastoral Staff, the Office Staff and Ministry Leaders to complaints, criminal charges and/or bad publicity. Any failure by a personnel of the Church to comply with the PDPA may lead to disciplinary action for serious or repeated breaches and/or a report being made to the Police, the Personal Data Protection Commission (the "Commission") and any other relevant government authority.

OVERVIEW OF THE PDPA

2. The PDPA came into effect on 2 January 2013 with the main personal data protection provisions coming into force on 2 July 2014. This document policy is formulated according to the following guidelines:
   a) Advisory Guidelines on Key Concepts in the Personal Data Protection Act (revised 27 July 2017)
   b) Advisory Guidelines for the Social Service Sector (updated 31 August 2018)
   c) Advisory Guidelines on the Personal Data Protection Act for NRIC and other National Identification Numbers (published on 31 August 2018)
   d) Advisory on Collection of Personal Data for Coronavirus Disease 2019 (COVID19) Contact Tracing and Use of Safe Entry (Dated 24th April 2020)
   e) Phase Three (Heightened Alert) – Precautionary Measures for Religious Activities first issued on 11th June 2021 and updated on 18th June 2021

3. **Purpose**

3.1 The PDPA is concerned with the protection of "Personal Data", which is defined as any data, whether true or not, about an individual who can be identified from that data or from that data and other information that an organisation has access to. The PDPA seeks to balance the rights of an individual to protect his/her personal data and the needs of organisations to collect, use and disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances.

4. Business Contact Information

4.1 The PDPA does not apply to "Business Contact Information", such as an individual's name, position or title, business telephone number and fax number, business address, business email address and any other similar information about the individual, which was given for commercial purposes or for a non-personal purpose.

4.2 However, if a person gives his Business Contact Information to the Church to receive goods or services from the Church for his personal purposes (in other words, he/she wants the Church to contact him/her at his/her office rather than his/her home), then the business contact information of that person will be personal data for the purposes of the PDPA.

OBLIGATIONS UNDER THE PDPA

5. Consent for Collection, Use or Disclosure of Personal Data

5.1 We will obtain the consent of our members, regular worshippers and visitors (collectively "**Congregants**") before we collect, use or disclose their personal data. In obtaining consent, we will use reasonable efforts to ensure that the Congregant is advised of the identified purposes for which his/her personal data is being collected, used or disclosed. Purposes will be stated in a manner that can be reasonably understood by the Congregant.

5.2 We will seek consent to use and disclose personal data at the same time as we collect the personal data. If we intend to use or disclose the personal data for a new purpose that was not previously identified, we will seek consent to use and disclose the personal data before it is used or disclosed for the new purpose.

5.3 We will collect personal data directly from Congregants, but we may also collect personal data from other sources including relatives or personal references or other third parties provided they have the right to disclose such personal data.

5.4 We will limit the type of personal data collected to that which is necessary for the purposes that we have identified.

5.5 A Congregant may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. A Congregant may contact us for more information regarding the implications of withdrawing consent.

5.6 In certain circumstances, personal data can be collected, used or disclosed without the consent of the individual. For example:

(a) the collection, use or disclosure is necessary for any purpose that is clearly in the interest of the individual, if consent for its collection, use or disclosure cannot be obtained in a timely way or the individual would not reasonably be expected to withhold consent, such as when the individual is seriously ill or mentally incapacitated;

(b) the collection, use or disclosure is necessary to respond to an emergency that threatens the life, health or safety of the individual or another individual;

(c) the collection, use or disclosure is necessary for any investigation or proceedings, if it is reasonable to expect that seeking the consent of the individual would compromise the availability or the accuracy of the personal data;

(d) the collection, use or disclosure is necessary for evaluative purposes;

(e) the personal data was provided to the Church by another individual to enable the Church to provide a service for the personal or domestic purposes of that other individual.

5.7 In compliance to the Advisory Guidelines on the Personal Data Protection Act for NRIC and other National Identification Numbers published on 31 August 2018, the Church will not collect, use or disclose the NRIC number or photocopy the NRIC of an individual unless required by:

a) The law or the authorities of the Government.
b) The Church to accurately establish or verify the identity of an individual to a high degree of fidelity.

Hence, we will continue to collect and use NRIC for the following purposes:

a) church membership and baptism
b) activities which involve travelling out of Singapore, hence the need for passport details and purchase of travel insurance and other logistics arrangement
c) other local activities, e.g., purchase of insurance for sports activities

6. Notification of Purpose

6.1 We will identify the purposes for which we collect, use or disclose personal data on or before we collect, use or disclose the personal data of Congregants. Upon receipt of the personal data, we will use or disclose the personal data only for the identified purpose and for purposes that a reasonable person would consider appropriate in the circumstances.

6.2 As a religious organisation, we generally collect, use and disclose personal data for the following purposes:

(a) To identify our members and those who regular worship with us and visitors to the Church;
(b) To carry out the ministry programmes and activities of the Church;
(c) To manage the administration and operations of the Church;
(d) To establish and maintain responsible relationships among Congregants; and
(e) To meet our legal and regulatory obligations.

6.3 When personal data that has been collected is to be used or disclosed for a purpose not previously notified, the new purpose will be notified to Congregants prior to use. Unless the new purpose is permitted or required by law, consent will be required before the personal data will be used or disclosed for the new purpose.

7. Use of Existing Personal Data

7.1 Personal data collected prior to 2 July 2014, when the main provisions of the PDPA on the protection of personal data came into force, can continue to be used or disclosed but only for the purpose that the personal data was originally collected, unless a Congregant has withdrawn his/her consent for such continued use or disclosure of his/her personal data.

7.2 If there is a new purpose for the use or disclosure of existing personal data, a fresh consent has to be obtained from the Congregants for this new purpose.

8. Disclosure of Personal Data

8.1 Generally, only ministers, elected office bearers, working committee members and office staff, with a need to know or whose duties or services reasonably require access to personal data are granted access to personal data about the Congregants of the member churches of the True Jesus Church Coordination Board (Singapore).

8.2 As a member of the True Jesus Church Coordination Board (Singapore), we may, however, disclose personal data of the Congregants to the relevant Board of Ministers and True Jesus Church Coordination Board (Singapore) Council Members in order for each of us to fulfil our respective roles and responsibilities as constituents of the True Jesus Church in Singapore.

9. Access to Personal Data

9.1 Upon receipt of a request from a Congregant, we will provide the Congregant with a reasonable opportunity to review the personal data that we have about the Congregant in our possession or under our control. Personal data will be provided within a reasonable time and at minimal cost to cover administrative expenses.

9.2 Upon receipt of a request from a Congregant, we will provide an account of the use and disclosure of the personal data of the Congregant. In providing an account of disclosure, we will provide a list of the organisations to which we may have disclosed personal data about the Congregant.

9.3 In certain situations, we may not be able to provide access to all of the personal data we hold about a Congregant; for instance:

(a) If doing so would likely reveal personal data about another individual or could reasonably be expected to threaten the life or security of another individual;
(b) If doing so would reveal any confidential information;
(c) If the information is protected by legal privilege;
(d) If the information was generated in the course of a formal dispute resolution process; or
(e) If the information was collected in relation to the investigation of a contravention of a law or a breach of an agreement.

9.4 In such a case, we will provide the reasons for denying access to the personal data.

10. Accuracy and Correction of Personal Data

10.1 We will endeavor to ensure that the personal data collected will be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used. Ensuring that the personal data that we possess is sufficiently accurate, complete and up-to-date will help minimize the possibility that inappropriate decisions are being made based on inaccurate or incomplete or outdated information.

10.2 We will promptly correct or complete any personal data found to be inaccurate or incomplete. Upon receipt of a request from a Congregant to correct or update his/her personal data, we will promptly correct or update his/her personal data.

10.3 Where we are not able to confirm the accuracy or completeness of a Congregant's personal data (such as those Congregants who have emigrated or who are no longer contactable), a note will be made against that Congregant's personal data of potential unresolved differences.

10.4 Where appropriate, we will inform third parties having access to the personal data in question of any amended personal data or the existence of any unresolved differences.

10.5 We will conduct an exercise periodically to update the personal data of the Congregants.

11. Transfer of Personal Data Outside of Singapore

11.1 We will protect personal data disclosed to third parties by contractual or other means stipulating the purposes for which it is to be used and the necessity to provide a comparable level of protection.

11.2 We will not transfer any personal data to any organisation located in a country or territory outside Singapore unless that other organisation is subject (whether by way of legislation or contractual arrangement) to obligations of protection of personal data that are comparable to those under the PDPA.

12. Security

12.1 We have the responsibility under the PDPA to make reasonable security arrangements to protect the personal data that we possess or control to prevent unauthorised access, collection, use, disclosure or similar risks.

12.2 We will use appropriate security measures to protect personal data against such risks as loss or theft, unauthorised access, disclosure, copying, use, modification or destruction, regardless of the format in which the personal data is held.

12.3 We operate close circuit television (CCTV) cameras in the Church premises for security and operational purposes. Except for security purposes, we do not use these CCTV cameras to identify an individual personally.

13. Retention and Destruction

13.1 We will keep personal data only as long as it remains necessary or relevant for the identified purposes or as required by law.

13.2 Once the personal data in our possession or control is no longer necessary for administrative or legal purpose, we will destroy or erase the personal data or remove the means by which the personal data can be associated with particular individuals (such as by way of anonymising the personal data).

14. Complaints

14.1 We will attend to and investigate any complaints concerning any possible breach of this Policy. If a complaint is found to be justified, we will take appropriate measures to resolve the complaint including, if necessary, amending our policies and procedures. The complainant will be informed of the outcome of the investigation regarding his/her complaint.

15. Handling of Personal Data of Church Staff

15.1 The personal data of Pastoral Staff and Office Staff, whether permanent or temporary, (collectively "**Church Staff"**) will be used only for purposes connected with their employment with the Church and for as long a period as is necessary following the termination of their employment.

15.2 We value the privacy of our Church Staff and shall process the personal data of our Church Staff in a fair and lawful manner. We will endeavour to comply with the obligations under the PDPA on the use of personal data in an employer-employee relationship.

15.3 From time to time, we may need to disclose some information held about Church Staff to government agencies, such as the Ministry of Manpower and the Central Provident Fund Board, and other relevant third parties, such as insurers, medical clinics and hospitals, solely for purposes connected with managing the employment of the Church Staff and providing for his/her welfare during his/her employment with the Church.

16. Appointment and Duties of the Data Protection Officer

16.1 The Church is required, as part of its compliance with the PDPA, to designate at least one person as its Data Protection Officer ("**DPO**").

16.2 It should be noted that the designation of a DPO does not relieve the Church of its legal obligations under the PDPA.

Responsibilities of the DPO

16.3 The DPO is responsible for ensuring that the Church complies with the PDPA. The DPO must keep fully up to date with the requirements of the PDPA and ensure that all personnel who handle personal data are fully aware of these requirements.

16.4 Where appropriate, the DPO may delegate some of his responsibilities as DPO to other individuals to ensure that the Church complies with the PDPA.

16.5 In addition to ensuring that the Church complies with the PDPA, the DPO is also responsible for dealing with queries and requests from individuals in relation to the Church's data protection policies and practices.

17. Data Breach Management

17.1 Should there be a breach of data, the Data Protection Officer (DPO) will activate the Data Breach Management Plan as detailed below:

Step	Action	Responsibility
a	Report data breach to the DPO via email with the following details: a) Date and time of the breach b) Person who reported the breach c) Description of the nature of the data breach	DPO
b	Fact Findings Initiate meeting (through phone, email or face to face) with the person who reported the case to collect tangible evidence of the case a) Cause of the data breach and whether the breach is still ongoing b) Number of affected individuals c) Type(s) of personal data involved d) The affected systems, servers, databases, platforms, services etc. e) Whether help is required to contain the breach f) The remediation action(s) that the organisation has taken or needs to take to reduce any harm to affected individuals resulting from the breach	DPO and Person reporting the breach
c	DPO will report the breach to the data breach management team. If it is necessary, the exco will be informed.	DPO and data breach management team
d	Contain the data breach to prevent further compromise of data and implement mitigating action(s) to minimise potential harms from the breach after an initial appraisal has been conducted to determine the extent of the breach.	DPO and data breach management team

e	Assess the data breach to determine the root cause (where possible) and the effectiveness of containment action(s) taken thus far to contain the data breach. Where necessary, continuing efforts should be made to prevent further harm from the data breach.	DPO and data breach management team
f	Report the data breach to: a) The PDPC (mandatory if the breach is a notifiable data breach under the Personal Data Protection Act ("PDPA")) no later than three calendar days. This includes data breaches that involve the personal data of 500 or more individuals or data breaches that may cause significant harm to individuals. b) The affected individuals (if required under the Data Breach Notification Obligation ("DBN Obligation")) as soon as practicable, at the same time or after notifying the PDPC. This includes data breaches that may cause significant harm to individuals.	DPO and data breach management team
g	Evaluate the organisation's response to the data breach and consider the actions that can be taken to prevent future data breaches. Where necessary, continuing efforts should be made to prevent further harm from the data breach.	DPO and data breach management team

18. Enquiries

18.1 For enquiries about the **True Jesus Church (Telok Kurau)** Policy, please write to the DPO at the following address:

32 Lor H Telok Kurau, Singapore 426020

Or email us at:

telok.kurau@tjc.org

19. Updating the Policy

19.1 This Policy may be updated from time to time to take account of changes in policy, technology, and/or to ensure compliance with any legislative changes.