Toa Payoh Methodist Church

PERSONAL DATA PROTECTION POLICY

Version 1.0 10 August 2014

TABLE OF CONTENTS

A. Management of Personal Data in Toa Payoh Methodist Church

A1. Introduction

1.1 In Toa Payoh Methodist Church, members' and visitors' personal data are collected and used for various Ministries and church activities. With the implementation of the Personal Data Protection Act (PDPA) coming into effect on 2 Jul 14, a data protection regime to govern the collection, use and disclosure of personal data is necessary to comply to the Act as well as to maintain individuals' trust and confidence in the Church that handle these data.

A2. Objective

2.1 To ensure that Toa Payoh Methodist Church is in compliance with the PDPA in the collection, use, disclosure, maintaining accuracy, handling and security of personal data in a manner that recognizes both the right of individuals to protect their personal data and the need of the Church to collect, use and disclose personal data for the purpose of maintaining the membership records and/or planning of Church/Ministries activities.

2.2 This policy defines the responsibilities of Toa Payoh Methodist Church in ensuring compliance to the PDPA by ensuring proper management, security control and supervision in the collection, usage and disclosure of the personal data in Church.

A3. Definition

3.1 The Personal Data Protection Act (PDPA) establishes a data protection law that comprises various rules governing the collection, use, disclosure and care of personal data. It recognizes both the rights of individuals to protect their personal data, including rights of access and correction, and the needs of organisations to collect, store, maintain accuracy, use or disclose personal information for legitimate and reasonable purposes.

3.2 Personal data refers to data, whether true or not, about an individual who can be identified from that data; or from that data and other information to which the organization has or is likely to have access. This includes names, contact numbers, addresses, pictures and videos to other types of data that do not directly identify an individual on its own but form part of an accessible record about an individual, whether the data is stored in electronic or non-electronic form.

3.3 Personal data in Singapore is protected under the Personal Data Protection Act 2012.

A4. Concept

4.1 The PDPA is intended to set the minimum standards that all organisation[1] in Singapore must observe. The PDPA will operate concurrently with other sectoral legislative and regulatory framework. This means that Church will have to comply with the PDPA as well as the common law and other relevant policies stipulated by the Methodist Church Of Singapore, when handling personal data in their possession.

4.2 The PDPA takes into account the following concepts:

4.2.1 Consent – Church may collect, use or disclose personal data only with the member's knowledge and consent (with some exceptions);

4.2.2 Purpose – Church may collect, use or disclose personal data in an appropriate manner for the circumstances, and only if they have informed the member of purposes for the collection, use or disclosure;

4.2.3 Reasonableness – Church may collect, use or disclose personal data only for purposes that would be considered appropriate to a reasonable person in the given circumstances.

A5. Data Protection Officer

5.1 The appointment of the Data Protection Officer is accountable to the Pastor-In-Charge and be responsible for ensuring that the Church complies with the PDPA. The appointed staff is responsible to review the Church's personal data policies with the Governance Committee and oversee the compliance of the PDPA. His or her responsibilities may include the following:

5.1.1 Develop processes for handling personal data in electronic and/or manual form, that suit the Church's needs and comply with the PDPA;

5.1.2 Communicate Church's internal personal data protection policies and processes to staff and members;

[1] The PDPA applies to all organisations which includes any individual, company, association or body of persons, corporate or unincorporated as well as charities, Institutions of a Public Character (IPC).

5.1.3 Handle queries or complaints about personal data from staff, members and visitors;

5.1.4 Alert Pastor-In-Charge, LCEC Chairman and Governance Committee Chairperson to any risks that might arise with personal data;

5.1.5 Liaise with General Conference (GC) and/or the Personal Data Protection Commission (PDPC), when required.

A6. Consent, Purpose Limitation and Notification Obligations

6.1 Collection of Personal Data

All registration forms are to provide a clause or separate notice to clearly state and seek consent for the following:

6.1.1 The purpose for the collection of data collected.

6.1.2 The usage of the data collected.

6.1.3 The ways the personal data may be disclosed.

The Privacy Clause and Consent to use of personal data is found in Appendix A.

6.2 Provision for Withdrawal of Consent

Toa Payoh Methodist Church will upon written request for withdrawal of consent, archived the information and will not use the information until consent is given. The request will be processed within 2 weeks.

A7. Accuracy Obligation

7.1 Toa Payoh Methodist Church will ensure that the data collected is accurate and complete; when in doubt, a request will be made to the individual for a verbal or written declaration that the personal data provided is accurate and complete.

7.2 Toa Payoh Methodist Church will ensure that personal data is updated and amended when requested.

A8. Protection Obligation

8.1 Confidentiality

Toa Payoh Methodist Church will ensure that all personal data is kept confidential and accessible only by the Data Protection Officer or authorized personnel for the purposes for which that information was sought.

8.2 Church Office

8.2.1 All staff working areas must be secured including work stations, meeting/ discussion areas, filing cabinets, printers and fax machines. Access to work areas must be limited by appropriate security measures.

8.2.2 Access to office equipment containing such information must be password locked.

8.3 Databases and registration files/forms

8.3.1 Soft copy databases must be password protected where applicable and stored by the dedicated Ministries during planning and destroyed when the information is no longer required after the activity.

8.3.2 Hardcopy registration files/forms containing personal information must be kept strictly under the Ministries' care during planning and destroyed when the information is no longer required after the activity.

8.3.3 Access to soft copy databases and hard copy files should only be given to authorized staff of the Church Office.

8.3.4 All staff are not allowed to save any copies of databases in their own computer hard drives or portable storage devices.

A9. Disclosure to Third-Parties

9.1 Toa Payoh Methodist Church will only disclose personal data to third parties only on a need-to-know basis for the purposes that the personal data have been collected for.

9.2 Third parties will be required to sign a confidential clause that will protect the personal data released and an agreement that the personal data will only be used for the purpose that it had been released.

A10. Retention Limitation Obligation

10.1 Toa Payoh Methodist Church will will retain and maintain its personal data records for the purpose of engagement, operational planning of activities, as well as communication of events, programmes and church-related information.

A11. Openness Obligation

11.1 Request

Toa Payoh Methodist Church will make information on data protection policies, practices and complaints processes available upon written request addressed to the Data Protection Officer.

11.2 Feedback

11.2.1 All feedback must be documented in the Feedback Record and submitted to the Pastor-In-Charge, LCEC Chairman and Governance Committee Chairperson.

11.2.2 The response to the query must be carried out within 5 working days, upon receiving the feedback.

11.2.3 Follow-up action must be carried out within reasonable time.

A12. Access Obligation

12.1 Requests for information on ways of usage and disclosure of their data.

12.1.1 For queries by telephone, staff must perform the following verification checks on the requester before disclosure of personal information:

- Full name as in NRIC
- NRIC/FIN number
- Home Address
- Contact number
- E-mail address

12.1.2 For queries through email or post, staff must follow-up with a telephone call to verify the identity of the requester before disclosure of personal information.

12.1.3 Staff are to provide the requested information only on verification of identity.

APPENDIX A

Privacy Policy and Consent to Use of Data

By interacting with, submitting information to or signing up for any organized activity offered by Toa Payoh Methodist Church and her Ministries, you agree and consent to Toa Payoh Methodist Church collecting, using, disclosing and sharing amongst the relevant Ministries your personal data, for the purpose of engagement, operational planning of activities, as well as communication of events, programmes and church-related information. Toa Payoh Methodist Church respects personal data and privacy, and will only share such information with third parties on a required basis. Should you wish to withdraw or limit your consent, please write with full particulars to:

Data Protection Officer
Toa Payoh Methodist Church
480 Lorong 2 Toa Payoh
Singapore 319641

Or email to:
dataprotection@tpmc.org.sg

APPENDIX B

Personal Data Protection Checklist

This self-assessment checklist designed by the Personal Data Protection Commission is based on the personal data protection obligations underlying the Personal Data Protection Act 2012 (PDPA) and is designed to assist organization in reviewing its policies and to consider ways in which it can protect the personal data in its custody.

S/n	Checklist	Yes/No/Action Plan
I-III Consent, Purpose Limitation and Notification Obligations		
Collection of Personal Data		
1	Do you collect personal data about your employees or members?	
2	Do you have personal data inventory map on: • What personal data is collected and why? • Who collects it? • Where it is stored? • Who is disclosed to?	
3	When collecting personal data, do you clearly inform the individual the purpose(s) for which it will be collected, used or disclosed and obtain his/her consent?	
4	If you collect personal data from third parties, do you ensure that the third party has obtained consent from the individuals to disclose the personal data to you for your intended purposes?	
5	If you are engaging a data intermediary to collect, use or disclose personal data on your organisation's behalf, have you ensured that the data intermediary will take the necessary action to ensure that your organization will be in compliance with the PDPA?	*Not Applicable*
6	Is there a formal process for the withdrawal of consent by individuals in respect of the collection, use or disclosure of their personal data?	
7	If you intend to collect the personal data without consent, have you checked the provisions of the PDPA to understand when you may use personal data without consent?	

Use of Personal Data		
8	Do you limit the use of personal data collected to only purposes that you have obtained consent for?	
9	For personal data collected before 2 July 2014, are you using the personal data only for the purposes you have obtained consent for?	
10	If you intend to use the personal data without consent, have you checked the provisions of the PDPA to understand when you may use personal data without consent?	
Disclosure of Personal Data		
11	Do you limit the disclosure of personal data collected to only purposes that you have obtained consent for?	
12	If you intend to disclosure the personal data without consent, have you checked the provisions of the PDPA to understand when you may use personal data without consent?	
IV. Access & Correction Obligation		
13	Have you established a formal procedure to handle requests for access to personal data?	
14	Do you have a list of third party organisations to whom personal data was disclosed and for what purposes?	
15	If you are imposing an administrative fee for access requests, have you developed the fee structure?	*Not Applicable*
16	Have you established a formal procedure to handle correction requests of personal data?	
17	Have you established a formal procedure to send corrected personal data to third party organisations that personal data was disclosed within one year of the correction?	
18	Have you checked S21(3) and the Fifth and Sixth Schedules of the PDPA to understand when you are not required to provide access or correct personal data?	

V. Accuracy Obligation		
19	Do you make reasonable effort to verify that the personal data kept are accurate and complete (i) prior to any use to make a decision that affects the individual or (ii) prior to disclosure?	
VI. Protection Obligation		
20	Have you assessed the personal data protection risks within your organisation and put in place personal data security policies?	
21	Is the personal data that you hold adequately classified?	
22	Is the personal data kept in a secure manner?	
23	Do external parties have easy access to the personal data that you hold?	
24	Are there any remedial measures in place in the event of a breach?	
25	Do you conduct or schedule regular audits on the data protection processes within your organisation?	
26	Are there contractual provisions in place to ensure proper safeguards in respect of personal data disclosed to outsourced parties who will be processing personal data on your behalf?	
VII. Retention Limitation Obligation		
27	Is there regular data housekeeping?	
28	Do you remove personal data no longer needed for business or legal purposes?	
VIII. Transfer Limitation Obligation		
29	Do you put in place the appropriate contractual arrangements or binding corporate rules to govern the transfer of personal data overseas?	*Not Applicable*
IX. Openness Obligation		
30	Have you designated one or two individuals (who may be referred to as data protection officers) to be responsible for ensuring that the data protection policies and practices of your organisation are in compliance with the PDPA?	

31	Does your data protection officer(s) know his/her roles and responsibilities in ensuring personal data in your organisation's possession or control is well-protected?	
32	Is the business contact information of your designated data protection officer(s) made available to the public?	
33	Have you developed and implemented data protection policies for your organisation to meet its obligations under the PDPA? Are your organisation's data protection policies made available to the public?	
34	Have you developed a process to receive, investigate and respond to complaints that may arise with respect to the application of the PDPA?	
35	Is information on your organisation's complaint process made available on request?	
36	Have you communicated information about your organisation's data protection policies and practices to your employees, in particular, but not limited to, employees who are handling personal data?	
37	Do your employees know who to pass the requests to if it is not their responsibility to respond to such requests?	