Pentecost Methodist Church

Personal Data Protection Policy

Doc. ID:	PMC-1POL-04b
Document Name:	Personal Data Protection Policy
Document Version:	2.0
Document Effective Date:	5 December 2021
Document Ownership:	Data Protection Officer

Version History

Name / Ministry	Changes Made	Approved by	Version No.	Date
-	Initial release	LCEC	1.0	14 Jan 2015
-	Updated point on collection of NRIC	LCEC	1.1	12 Sep 2018
Maurice Lim / Governance	- Updated Policy to cover various obligations under the PDPA - Updated Policy to incorporate new amendments which took effect from 1 Feb 2021	LCEC	2.0	5 Dec 2021

Contents

1 INTRODUCTION

1.1 Purpose of Policy

This Policy is prepared by Pentecost Methodist Church ("PMC" or "the Church"). The Policy is approved by the Local Church Executive Committee ("LCEC").

PMC is committed to safeguarding the personal data collected by the Church. PMC seeks to manage the personal data of individuals in accordance with the Singapore Personal Data Protection Act 2012 (the "PDPA") and other applicable laws.

The PDPA establishes a data protection law that comprises various rules governing the collection, use, disclosure and care of personal data. It recognises both the rights of individuals to protect their personal data, including rights of access and correction, and the needs of organisations to collect, use and disclose personal data for legitimate and reasonable purposes.

This Policy outlines the principles and practices adopted by PMC to comply with the PDPA by ensuring proper management, security control and supervision in the collection, use and disclosure of individuals' personal data.

1.2 Policy Statement

Under the PDPA, PMC will inform the individual of the purposes for which his/her personal data will be collected, used or disclosed on or before such collection, use or disclosure and make reasonable security arrangements to protect personal data in its possession or under its control in order to prevent (a) unauthorized access, collection, use, disclosure, copying, modification or disposal, or similar risks; and (b) the loss of any storage medium or device on which personal data is stored. PMC will remove the personal data of individuals, as soon as the purpose for which that personal data was collected is no longer being served by retention of the personal data.

This Policy reflects PMC's endeavor to:

a. Take all necessary efforts to comply with the requirements of the PDPA and good practices;
b. Ensure that individuals' personal data are not misused;
c. Help, train and support staff and volunteers who handle personal data to understand the requirements of the Policy so that they can act confidently and consistently;
d. Respond to any legitimate enquiries from individuals regarding usage, storage and accuracy of their personal data in a timely manner.

2 KEY TERMS

Individual – Individual means a natural person, whether living or deceased.

Personal Data – Personal data means data, whether true or not, about an individual who can be identified from that data; or from that data other information to which PMC has, or is likely to have, access:

- Full name
- NRIC Number or FIN (Foreign Identification Number) or passport number
- Facial image or individual (photograph or video image)
- Personal mobile number
- Personal email address
- Residential address
- Residential telephone number
- Biometric identifiers (face geometry or fingerprints)

Excluded Personal Data – The PDPA does not apply to the following categories of personal data:

a. Personal data that is contained in a record that has been in existence for at least 100 years;
b. Personal data about a deceased individual who has been dead for more than 10 years; and
c. Business contact information, which is information not provided by an individual solely for personal purposes, and includes an individual's:
   - Name;
   - Business title;
   - Business telephone number; and

- Business address and email address

Collection – The term 'collection' refers to any act or set of acts through which PMC obtains control over or possession of personal data.

Use – The term 'use' refers to any act or set of acts by which PMC employs personal data. A particular use of personal data may occasionally involve collection or disclosure that is necessarily part of the use.

Disclosure – The term 'disclosure' refers to any act of set of acts by which PMC discloses, transfers or otherwise makes available personal data that is under its control or in its possession to any other organisation.

3 ACCOUNTABILITY OBLIGATION

Accountability is a fundamental principle of the PDPA which requires PMC to ensure and demonstrate compliance with the PDPA through proper management and protection of personal data.

PMC is answerable to regulatory authorities an individuals who entrust PMC with personal data, and will implement the necessary policies and procedures to fulfil its PDPA obligations. The PMC Personal Data Protection Policy is available on the PMC website at http://pmc.org.sg/info.

3.1 Data Protection Officer

PMC will appoint a Data Protection Officer ("DPO") who will be accountable to the Pastor-in-Charge and will work with all concerned parties including the Chairperson of the LCEC, Chairperson of Governance Committee and Church Office Manager/Administrator to ensure compliance of the PDPA.

The DPO is responsible to review PMC's personal data protection policy and oversee the compliance of the PDPA and his/her responsibilities include but may not be limited to the following:

a. Develop processes for handling personal data in electronic and/or manual form, that suit PMC's needs and comply with the PDPA;
b. Communicate PMC's internal personal data protection policy and processes to staff and members;
c. Handle queries or complaints about personal data from staff, members and visitors;
d. Alert Pastor-in-Charge and LCEC Chairman to any risks that might arise with personal data; and
e. Liaise with Trinity Annual Conference ("TRAC") and/or Personal Data Protection Commission ("PDPC") as required.

Any requests for personal data access or correction by individuals, including any enquiries and complaints may be submitted to PMC in writing to the DPO at the following contact information:

Pentecost Methodist Church
4 Pasir Ris Drive 6
Singapore 519420
Telephone: 6584 0297
Email: dpo@pmc.org.sg

4 COLLECTION OF PERSONAL DATA

4.1 Notification Obligation

PMC normally collects information on personal data directly from the individual.

PMC may collect individuals' information from other persons / organisations with their consent or as authorised by law.

PMC informs individuals of the purposes for which the information is collected before or at the time of collecting personal data.

All registration forms, application forms and pledge cards used by PMC must provide a clause or notice to clearly state and seek consent for the following:

a. The purpose for the collection of data collected;
b. The usage of the data collected;
c. The ways the personal data may be disclosed.

PMC will collect the data by fair and lawful means. These include but are not limited to:

a. Application forms or personal data submitted by an individual to PMC relevant to all events and activities organized or managed by PMC;
b. Where an individual contacts the staff or representatives of PMC to make enquiries or in relation to pastoral care or social aid, whether such contact is by email, voice calls or any other medium;
c. Where an individual makes a donation to PMC;
d. Where an individual submits his/her personal data for the purpose of employment;
e. Where an individual submits his/her personal data for the purpose of volunteering at PMC events, activities, programs or courses.

PMC will not retain the physical Identity Document of the individual but may collect and use the NRIC / Foreign Identification / Birth Certificate / Work Permit / Passport numbers or make copies of these documents when it is necessary to precisely verify an individual's identity to a high degree of fidelity. This may include the following purposes within the church's operations:

a. Pledge
b. Baptism
c. Membership
d. Mission / Church Camp
e. Marriage solemnization
f. Pre-employment application / employee appointment

4.2 Consent Obligation

PMC will ask for consent to collect, use or disclose an individual's personal data, except in specific circumstances where collection, use or disclosure without consent is authorised or required by law.

PMC may not be able to provide certain services if individuals are unwilling to provide consent to the collection, use or disclosure of certain personal data.

4.2.1 Deemed Consent

Deemed consent is a form of consent where consent is inferred or implied from the circumstances or the conduct of the individual that the individual does consent to the collection, use and disclosure of his personal data by his conduct, although he has not expressly stated his consent in written or verbal form.

PMC may deem that the individual's consent for the use of their personal data collected before 2 July 2014 for the purpose which it was collected, has been obtained unless consent has been withdrawn by the individual.

PMC may deem the individual's consent is obtained for the collection, usage and disclosure of their personal data when the individual signed up for specific activities organised by the Church such as membership application, ministry events / courses or voluntarily provided personal data for the purposes listed in Section 4.1 above.

PMC need not seek consent from their employees (including volunteers and part-time workers) for purposes related to their work in PMC. However, employee's consent shall be obtained if such purpose is unrelated to their work. Employees shall be informed that their personal data may be disclosed, and arrangements may be made to limit such disclosure with mutual agreement.

4.2.2 Deemed Consent by Notification (wef 1 Feb 2021)

An individual may be deemed to have consented to the collection, use or disclosure of personal data for a purpose that he had been notified of, and has not taken any action to opt out of the collection, use or disclosure of his personal data within a stipulated reasonable period.

PMC must, before collecting, using or disclosing any personal data about an individual, conduct an assessment to determine that the proposed collection, use or disclosure of personal data is not likely to have an adverse

effect on the individual. The assessment for relying on deemed consent by notification will also have to take into consideration the method of notification and opt-out period.

4.2.3 Withdrawal of Consent

Any individual may withdraw their consent to the use and disclosure of his/her personal data at any time, unless such personal data is necessary for PMC to fulfil its legal obligations.

PMC shall comply with the withdrawal request and inform the individual if such withdrawal will affect services or arrangements between the individual and the Church, and PMC may cease such services or arrangements as a result of the withdrawal.

4.3 Purpose Limitation Obligation

PMC will inform individuals of the purposes for which the information is collected before or at the time of collecting personal data, and the nature of information collected will be limited to only information relevant for the intended purpose.

5 CARE OF PERSONAL DATA

5.1 Accuracy Obligation

PMC shall make every reasonable effort to ensure that personal data collected and kept are accurate and complete. PMC relies on individuals' self-notification of any changes to their personal data that is relevant to PMC or affect services or arrangements with PMC.

Information voluntarily submitted by an individual to PMC shall prima facie be deemed complete and accurate.

5.2 Protection Obligation

PMC shall adopt security measures that are reasonable and appropriate to the circumstances, taking into consideration the nature of the personal data, the form in which the personal data is collected (physical or electronic) and the possible impact to the individual concerned if an unauthorized person obtained, modified or disposed of the personal data. These measures fall into 3 categories – technical, administrative and physical, with examples stated below.

5.2.1 Technical Measures

a. Securing PMC IT network from unauthorized access including access through the website;
b. Adopt appropriate access controls and authentication measures;
c. Ensure that portable electronic devices issued by PMC are password protected;
d. De-identifying / anonymizing such personal data before sharing with other general users, contractors, vendors or external partners and collaborators;
e. Activating self-locking mechanisms for the computer screen if the computer is left unattended for a certain period;
f. Installing appropriate computer security software and using suitable computer security settings that are updated regularly;
g. Disposing of personal data in IT devices that are to be recycled, sold or disposed;
h. Files containing sensitive or confidential data are in secured folders and only made available to staff with authorized access.

5.2.2 Administrative Measures

a. Include confidentiality obligations in code of conduct and employment agreements;
b. Regular training sessions for staff to impart good practices in handling personal data and strengthen awareness of threats to security of personal data;

c. Ensuring that only the appropriate amount of personal data is held, as holding excessive data will also increase the efforts required to protect personal data.

5.2.3 Physical Measures

a. Limiting access to physical areas where personal data is stored;
b. Storing hardcopies of confidential documents in locked file cabinet systems;
c. Restricting employee access to confidential documents on a need-to-know basis;
d. Ensuring proper disposal of confidential documents that are no longer needed, through shredding or similar means;
e. Providing a summary of personal data in storage so that personal data is accessed only when necessary;
f. Ensuring that the intended recipient of the personal data is the correct recipient to avoid undue disclosure of personal data.

5.3 Retention Limitation Obligation

PMC will retain the individual's personal data only as long as it is reasonable to fulfill the purposes for which the information was collected or for legal or business purposes.

PMC reviews the personal data that they hold on a regular basis to determine if that personal data is still required.

PMC may anonymise collected personal data, or destroy records containing personal data once the information is no longer needed.

PMC uses appropriate security measures when destroying personal data, including shredding paper records and permanently deleting electronic records.

5.4 Transfer Limitation Obligation

PMC may disclose individuals' personal data to the following internal and external organisations for appropriate purposes and subject to compliance of applicable laws:

a. TRAC, Methodist Church of Singapore ("MCS") General Conference, agents, contractors, data intermediaries or third-party service providers who provide services such as telecommunications, mailing, information technology, payment, payroll, training, storage and archival, to PMC;
b. Banks and financial institutions;
c. Professional advisers such as auditors;
d. Relevant government regulators, statutory boards or authorities or law enforcement agencies to comply with any laws, rules, guidelines and regulations or schemes imposed by any government authority;
e. Charity organisations; or
f. Any other relevant person in connection with the intended purposes.

PMC will take reasonable steps to check whether the recipient of the personal data is bound by legally enforceable obligations to provide the transferred data a standard of protection that is at least comparable to the PDPA's protections.

PMC may transfer personal data to a country or territory outside Singapore, when required for business purposes, using a secured mode of transfer, which is aligned with PDPA requirements.

6 INDIVIDUAL'S AUTONOMY OVER PERSONAL DATA

6.1 Access and Correction Obligation

Individuals whose personal data are kept by PMC may request for access to their personal data. Staff are to provide the requested information only upon verification of the identity of the inquirer and upon such reasonable conditions as PMC shall impose.

When an individual makes an access request on behalf of a third party or vice versa, he/she must have proof of consent from the respective individual, for the relevant purpose for which the request is made. For any other purpose, a separate consent must be obtained.

For queries by telephone, staff must perform the following verification checks on the individual requesting for information before disclosure of personal information:

- Full Name as in NRIC
- Last 3 numerical digits plus alphabet of NRIC/FIN Number
- Full Address
- Contact Number(s)
- Email Address

For queries through email or post, staff must follow up with a telephone call to verify the identity of the individual requesting for information before disclosure of personal data.

Any requests for personal data access or correction by individuals, including any enquiries and complaints may be submitted to PMC in writing to the DPO (see 3.1).

6.2 Data Breach Notification Obligation (wef 1 Feb 2021)

A data breach, in relation to personal data, refers to any unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data such as through hacking or the installation of ransomware. It also includes the loss of any storage medium or device on which personal data is stored in circumstances where the unauthorised access, collection, use, disclosure, copying, modification or disposal of the personal data is likely to occur. Disclosing personal data to a wrong recipient, where the individual whose personal data had been disclosed had not consented to such disclosure, is also considered a data breach.

A data breach can be the result of malicious activities, human error or computer system weakness. PMC will put in place measures which monitor and take pre-emptive actions to prepare for data breaches.

PMC will notify the PDPC of any data breach that:

a. Results in, or is likely to result in, significant harm to the affected individuals; or
b. Is of a significant scale (i.e., involves personal data of 500 or more individuals).

Affected individuals must be notified if the data breach is likely to result in significant harm to them. The PDPA provides a prescribed list of personal data or classes of personal data that shall be deemed to result in significant harm to affected individuals if compromised in a data breach, including authentication data relating to an individual's account with an organisation, credit card information, bank account number, creditworthiness of an individual, salary information etc.

PMC shall notify the PDPC (at https://eservice.pdpc.gov.sg/case/db) no later than 3 calendar days after the day it confirms that the data breach is a notifiable data breach. Notifications to affected individuals must be made as soon as practicable, at the same time or after notifying the PDPC.

7 POLICY REVIEW AND MONITORING

The DPO will from time to time work with PMC's Governance Committee to review and monitor compliance to this Policy.

The Policy shall be maintained and updated by the DPO and approved by the LCEC at a minimum once every two years, or earlier if triggered by any material change in circumstances or regulatory requirements.