Personal Data Protection Policy

The Fairfield Methodist Church, Singapore

---

21 July 2022 – Version 2.0

Contents

1. Policy information

Document Owner
Policy prepared by Fairfield Methodist Church (FFMC), Local Conference Executive Council (LCEC)
FFMC and Scope of policy
This policy applies to all staff, members and volunteers of Fairfield Methodist Church (FFMC), as well as its sub-contractors, if any. A copy of this policy shall be provided to any Individual upon request.
Policy operational date
August 2014
Date approved by the LCEC
August 2014

Revision Date	Version No	Description of Revision
21 July 2022	02	This policy replaces all previous PDPA policies which had no version control in place. Effective XX XXX 2022

2. Introduction

2.1. Purpose of policy

2.1.1. Fairfield Methodist Church (FFMC) is committed to safeguarding the personal data entrusted to it by Individuals.

2.1.2. FFMC manages Individuals' personal data in accordance with Singapore Personal Data Protection Act 2012 (PDPA) and other applicable laws.

2.1.3. This policy outlines the principles and practices FFMC follows in protecting personal data.

2.2. Definitions

2.2.1. Personal data

Personal data means 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 FFMC has or is likely to have access.

2.2.2. Individual

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

2.2.2.2. For FFMC, individuals can be categorized as follows:

2.2.2.2.1 FFMC staff (paid or not paid, including volunteers);

2.2.2.2.2 FFMC members and regular woshippers.

2.2.3. Purpose

The term "purpose" refers to objectives or reasons that FFMC has collected the personal data for.

3. Policy Statement

3.1. FFMC will:

3.1.1. comply with both the law and good practice;

3.1.2. respect Individuals' rights;

3.1.3. be open and honest with Individuals whose data is held;

3.1.4. provide training and support for staff and volunteers who handle personal data, so that they can act confidently and consistently.

3.2. FFMC recognizes that its first priority under the PDPA is to avoid causing harm to Individuals, viz:

3.2.1. keeping information securely in the right hands;

3.2.2. holding good quality information, and

3.2.3. destroying information as soon as retention is no longer necessary for legal or business purpose.

3.3. Secondly, the PDPA aims to ensure that the legitimate concerns of Individuals about the ways in which their data may be used are taken into account. In addition to being open and transparent, FFMC will seek to give Individuals as much choice as is possible and reasonable information over what data is held and how it is used.

4. Responsibilities

4.1. FFMC's LCEC Responsibilities

4.1.1. LCEC recognizes its overall responsibility for ensuring that FFMC complies with its following legal obligations:

4.1.1.1. Develop and implement its data protection policies and practices;

4.1.1.2. Nominate a Data Protection Officer (DPO);

4.1.1.3. Develop process to receive and respond to complaints that may arise with respect to the application of PDPA;

4.1.1.4. Communicate to FFMC staff information about its data protection policies and practices;

4.1.1.5. Make information available on request about FFMC's data protection policies and practices and its process to receive and respond to complaints;

4.1.2. Each FFMC ministry team where personal data is handled is responsible for drawing up its own operational procedures (including induction and training) to ensure that good Data Protection practice is established and followed.

4.2. FFMC Staff and Third-Party Responsibilities

4.2.1. All FFMC staff and third-parties (sub-contractors, vendors, suppliers, volunteers etc) are responsible for complying with the approved PDPA policy and supporting guidance.

4.2.2. All staff are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work with FFMC.

4.2.3. Where anyone within FFMC feels that it would be appropriate to disclose information in a way contrary to the PDPA policy, or where an official disclosure request is received, this will only be done with the authorisation of the DPO.

4.2.4. All such disclosures will be documented.

5. Data Collection, Usage and Disclosure

5.1. Purpose Limitation

5.1.1. FFMC collects, uses and discloses personal data for the purposes in connection with the services it provides to an Individual:

5.1.1.1. Staff Administration;

5.1.1.2. Event organisation and management;

5.1.1.3. Queries and requests handling;

5.1.1.4. Meeting regulatory requirements;

5.1.1.5. Advertising and communication.

5.1.2. Whenever data is collected, the number of mandatory fields will be limited to only that information relevant to the purpose, and Individuals will be informed which fields are mandatory and why.

5.2. Consent

5.2.1. FFMC 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 authorized or required by law.

5.2.2. In situations where FFMC cannot conveniently obtain consent from an Individual in writing by signing a consent form, by checking a box on a form, or electronically by clicking a button, FFMC may opt to obtain verbal consent (in person, by telephone). Such consent shall be documented in writing as soon as is practicable.

5.2.3. FFMC 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.

5.3. Deemed Consent

5.3.1. Deemed consent is a form of consent where consent is inferred or implied from the circumstances or the conduct of the Individual and 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.

5.3.2. Deemed Consent By Conduct

Deemed consent by conduct applies to situations where the individual voluntarily provides his personal data to the organisation. An individual may be regarded as voluntarily providing personal data where the individual takes certain actions that allow the data to be collected, without providing the data himself. Consent is deemed to be given to the extent that the individual intended to provide his personal data and took the action required for the data to be collected by FFMC.

5.3.3. Deemed Consent By Contractual Necessity [wef 01 Feb 2021]

FFMC may assume Individuals have given consent in cases where they provide personal data where it is reasonably necessary for FFMC to process and disclose the information collected to third party(ies) in order to perform and conclude a transaction requested by the Individuals.

5.3.4. Deemed Consent By Notification [wef 01 Feb 2021]

5.3.4.1. 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 he has not taken any action to opt out of the collection, use or disclosure of his personal data within a stipulated reasonable period.

5.3.4.2. FFMC 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.

5.3.5. FFMC may assume Individuals have given consent in cases where they volunteer information for an obvious purpose.

5.3.6. FFMC may continue to use personal data collected before 2nd July 2014 for the purpose which it was collected, unless consent has been withdrawn by the Individual.

5.3.7. Consent will normally not be sought for most processing of information about employees (staff and volunteers), with the following exceptions:

5.3.7.1. Staff (including volunteers) details will only be disclosed for purposes unrelated to their work for FFMC with their consent;

5.3.7.2. Staff (including volunteers) working from home, will be given the choice over which contact details are to be made public.

5.3.8. In case of information provided by other churches on their staff and members to FFMC, FFMC may assume that the church has fully explained to these Individuals that their personal information has been provided to FFMC, the items of the information collected, purposes of the information collection, process and use, and has obtained their written consent for the disclosure of the said information to FFMC.

5.4. Consent Withdrawal

5.4.1. An Individual may withdraw consent to the use and disclosure of personal data at any time by giving reasonable notice, unless the personal data is necessary for FFMC to fulfil its legal obligations.

5.4.2. FFMC will respect his decision, but may not be able to provide him with certain products and/or services if it does not have the necessary personal data.

5.4.3 The notice to withdraw consent should be submitted to the DPO.

5.5. Notification Obligation

5.5.1. FFMC normally collects information on personal data directly from the Individual.

5.5.2. FFMC may collect Individuals' information from other persons/organisations with their consent or as authorized by law.

5.5.3. FFMC will notify Individuals, before or at the time of collecting personal data, of the purposes for which the information is collected.

5.5.4. FFMC does not provide this notification when an Individual volunteers information for an obvious purpose (Example: when completing a registration form to participate to a retreat and the data is not used for another purpose than managing and organizing the event), or when the Individual is deemed to have consented to the collection, use or disclosure of his personal data (see paragraph 5.3.4 above).

5.6. Accuracy Obligation

5.6.1. FFMC makes every reasonable effort to ensure that the Individuals' information it keeps is accurate and complete.

5.6.2. Information voluntarily submitted by an Individual to FFMC shall prima facie be deemed complete and accurate. Where the currency of the personal data is important, FFMC may take steps to verify that the information submitted by an Individual is up to date.

5.6.3. Individuals remain primarily responsible and liable to ensure that all personal data submitted to FFMC is complete and accurate. They are to notify FFMC of any change to their personal data that was submitted to FFMC.

5.7. Data Disclosure and Transfer of Personal Data Outside Singapore

5.7.1. FFMC may disclose Individuals Personal Data to the following group of external organisations for purposes mentioned above (see paragraph 5.1), subject to the requirements of applicable laws:

5.7.1.1. 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 FFMC;

5.7.1.2. banks and financial institutions;

5.7.1.3. Professional advisers such as auditors;

5.7.1.4. 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;

5.7.1.5. Charity organisations;

5.7.1.6. any other person in connection with the purposes set forth above.

5.7.2. FFMC will take appropriate steps to check whether, and ensure that, 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.

5.7.2. FFMC 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. Security and storage

6.1. Protection Obligation

FFMC has adopted security arrangements 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.

6.1.1. Storage of Personal Data

FFMC is implementing reasonable and appropriate security measures to protect the storage of personal data such as:

6.1.1.1. Marking confidential documents clearly and prominently;

6.1.1.2. Storing hardcopies of confidential documents in locked file cabinet systems;

6.1.1.3. Storing soft copies of confidential documents in secured folders;

6.1.1.4. Archived paper records and data backup files may be stored securely off-site.

6.1.2. Protection of Personal Data

6.1.2.1. All personal and sensitive personal data held will secured against unauthorised access and theft.

6.1.2.2. FFMC will ensure that:

a) FFMC's IT network is as secure as possible from unauthorised access including access through the website;
b) Individual PCs are password protected;
c) Personnel and other files holding sensitive or confidential personal data are secured and only made available to staff with authorised access;
d) Ensuring that IT service providers are able to provide the requisite standard of IT security;
e) FFMC will notify the PDPC, without delay, of a security breach affecting personal data if it creates a real risk of significant harm to Individuals.

6.2. Retention Limitation Obligation

6.2.1. FFMC retains member's personal data only as long as it is reasonable to fulfil the purposes for which the information was collected or for legal or business purposes.

6.2.2. FFMC reviews the personal data that it holds on a regular basis to determine if that personal data is still required.

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

6.2.4. FFMC uses appropriate security measures when destroying personal data, including shredding paper records, returning the documents to the Individuals concerned, and permanently deleting electronic records.

7. Access and correction of personal data

7.1. Access to Personal Data

Under the PDPA, an Individual has the right of access to his personal data in FFMC or under FFMC's control or information which may have been used or disclosed by FFMC, within a year before the date of his request.

7.2. Correction of Personal Data

7.2.1. Keeping an Individual's personal data accurate and updated is very important to FFMC. Individuals can help FFMC keep accurate records by informing FFMC of any changes, errors or omissions in their personal data.

7.2.2. FFMC will implement correction of the personal data as soon as practicable; and send the corrected personal data to all other external organisations to which the personal data was disclosed by FFMC within a year before the date the correction was made, unless that other organisation does not need the corrected personal data for any legal or business purpose with FFMC.

7.3. Access and Correction Process

7.3.1. The DPO will oversee the handling of any requests for personal data access or correction.

7.3.2. All FFMC staff are required to pass on any personal data access or correction requests to the DPO, as soon as possible.

7.3.3. Requests for personal data access or correction must be submitted to FFMC in writing.

7.3.4. Those making a personal data access or correction request may be asked by FFMC to provide additional information which will help to process the request. Where applicable, a fee may be charged to process an access request in order to recover the incremental costs of responding to the access request.

7.3.5. The DPO shall verify the identity of the Individual before responding to the request for access or correction.

7.3.6. In the case of access request to personal data, the relevant data will be provided a format or using a method determined by FFMC.

7.3.7. FFMC's contact with regard to any inquiries, complaints, access/correction of personal data, is FFMC's DPO with the following contact information:

FFMC DPO Tel XXXX-XXXX

dpo@ffmc.org.sg

7.4. Accountability Obligation

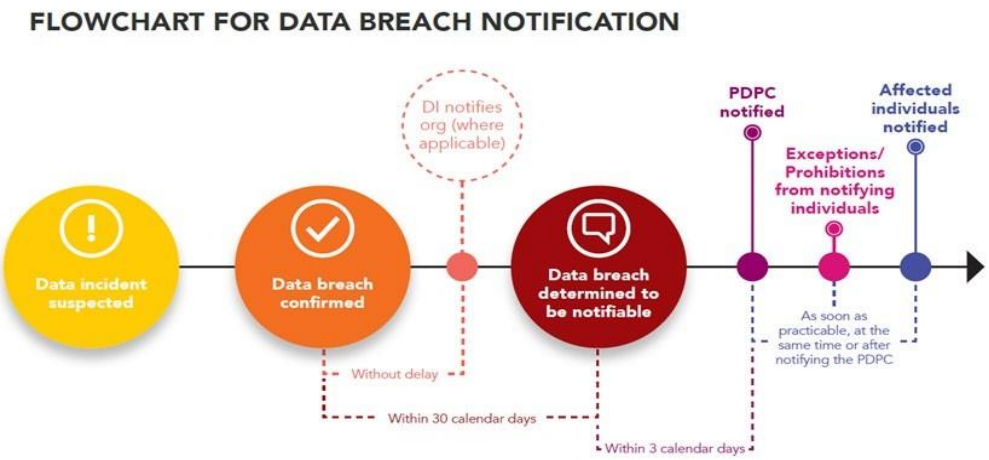
FFMC's Personal Data Protection Policy is made available on request.

8. Data Breach Notification Obligation [wef 01 Feb 2021]

8.1. 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, and the Individual whose personal data had been disclosed had not consented so such disclosure is also considered a data breach.

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

8.3. A data breach management plan (DBMP) as described below will enable FFMC to respond swiftly by managing any data breaches in a systematic manner.



8.4 Data Breach Notification Process

8.4.1 The Data Breach Management Team (DBMT) will manage any data breach notifications.

8.4.2 The DBMT will comprise:

- LCEC Chair
- LCEC Vice Chair
- Lay Leader
- Pastor in Charge
- DPO

8.4.3 Any suspicion of a potential or real data breach is to be submitted to the DBMT as soon as possible, for assessment of risk and to establish the root cause of the breach and its severity on FFMC and the affected Individuals

8.4.4. The DBMT will undertake to identify, prepare and respond to data breaches by carrying out the following steps (C.A.R.E) –

8.4.4.1. **C**ontain 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.

8.4.4.2. **A**ssess the data breach by gathering the facts to determine the root cause (where possible) and assessing the effectiveness of containment action(s) taken thus far to contain the data breach before processing to implement full remedial actions. Where necessary, continuing efforts will be made to prevent further harm from the data breach.

8.4.4.2.1. DBMT will assess whether a data breach is notifiable and notify the affected individuals and/or the Commission where it is assessed to be notifiable.

8.4.4.2.2. If FFMC has suffered a data breach that has:

(i) caused (or is likely to cause) significant harm to affected Individuals. Significant harm" could include physical, psychological, emotional, economic and financial harm, as well as harm to reputation and other forms of harms that a reasonable person would identify as a possible outcome of data breach.

(ii) affected at least 500 Individuals then it generally must inform the Personal Data Protection Commission (PDPC) and affected Individuals of the breach.

8.4.4.3. **R**eport the data breach to:

(i) PDPC at https://eservice.pdpc.gov.sg/case/db in the event the breach suffered is a notifiable breach.

Notification is to be done to the PDPC no later than 3 working days after the day FFMC makes the assessment that a data breach is a notifiable data breach.

(ii) The affected individuals as soon as is practicable.

8.4.4.4. **E**valuate FFMC's response to the data breach and consider the actions that can be taken to prevent future data breaches. Where necessary, continuing efforts will be made to prevent further harm from the data breach.

9. Policy Review

9.1. The Personal Data Protection Policy shall be maintained and updated by the DPO

9.2. This review shall take place annually by the Governance Subcommittee, and any revisions approved by the FFMC Local Conference Executive Committee.