Personal Data Protection Policy

Agape Methodist Church

30 March 2015 – Version 1.0

Contents

Policy Information

Document Owner
This policy was prepared by Agape Methodist Church.
Organisation and Scope of policy
This policy applies to all the staff, including lay and clergy office bearers of Agape Methodist Church. A copy of this policy will be made available to any individual upon request.
Policy operational date
{21/04/2015}
Date approved by Agape Methodist Church, Local Church Executive Committee
{21/04/2015}
Policy review date
{30/03/2015}

1. Introduction

1.1 Purpose of Policy

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

In Agape Methodist Church (Church), individuals' personal data are collected and used for its various ministries and church activities. With the implementation of the Personal Data Protection Act (PDPA) which came into effect on 2 July 2014, this personal data protection policy (Policy) outlines the principles and practices that governs the Church in protecting personal data collected for its use.

1.2 Objective

To ensure that the Church is in compliance with the PDPA in the collection, use, disclosure, and care of personal data in a manner that recognises both the rights of individuals to protect their personal data, including rights of access and correction, and the needs of the Church to collect, use and disclose personal data for its ministry, activities and other reasonable related purposes.

This Policy defines the responsibilities of the 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 the Church.

1.3 Definitions

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 Church has or is likely to have access. It includes information such as personal particulars, medical records, educational records, financial records, etc., whether the data is stored in electronic or non-electronic form.

For the Church, individual refers to a natural person, whether living or deceased, that includes but not limited to the following:

- Staff (either paid or not paid. Unpaid staff include volunteers, lay person holding office or represents the Church in anyway.)
- Members
- Donors
- Beneficiaries
- Prospects
- Visitors

2. Responsibilities

2.1 Local Church Executive Committee's responsibilities

The Local Church Executive Committee (LCEC) is the responsible authority for ensuring that the Church complies with the implementation of its data protection policies and practices set out in this Policy which includes the following:

- Appoint Data Protection Officer(s)
- Review and approve the Policy and any updates, amendments, etc., for its implementation
- Review and approve the process to receive and respond to complaints that may arise with respect to the application of the Policy
- Ensure communication of the Policy to its staff and other parties who handle data collected on behalf of the Church

2.2 Data Protection Officer's responsibilities

The appointed Data Protection Officer(s) (DPO) is/are responsible to review the Policy with the Governance Committee to ensure compliance with the PDPA and oversee the compliance of the Policy. The responsibilities include but are not limited to the following:

- Develop processes to manage personal data in electronic and/or manual form, that suit the Church's needs in compliance with the Policy
- Communicate the Church's internal personal data protection practices and processes to staff and members
- Develop processes to handle queries including requests for access or correction to or complaints about personal data that may arise from the implementation of the Policy
- Alert Pastor-In-Charge, LCEC Chairperson and Governance Chairperson to any risks that might arise with personal data
- Liaise with General Conference (GC) and/or the Personal Data Protection Commission (PDPC), when required
- Recommend any implementation processes

2.3 Staff's and ministries'/committees' responsibilities

Each Church ministry/committee is responsible for formulating their respective operational procedures in compliance to this Policy (including induction and training) to ensure that good data protection practices are established and implemented.

All Church Staff, paid and unpaid, including lay and clergy office bearers, who manage personal data are to comply with this Policy. They are to read, understand and acknowledge the policies and procedures that relate to the personal data that they manage in the Church.

Staff are to seek approval from the DPO in the occasion that there is a need to consider using personal data in a manner not consistent with this Policy, or an official disclosure request is received. The considerations, approval and processes of the disclosures are to be documented and filed.

Significant breaches of this Policy will be referred to according to the Church's disciplinary procedures.

3. Data Collection, Usage and Disclosure

3.1 Purpose limitation

The Church may collect personal data relevant to the purpose of the collection and for purposes that would be considered appropriate to a reasonable person in the given circumstances.

Prior to or during collection of personal data, the Church must make known to the individual and seek consent for the following:

- The purpose for which the personal data was collected;
- The usage of the personal data collected; and
- The ways the personal data may be disclosed.

3.2 Consent

The Church may collect, use or disclose personal data only with the individual's knowledge and consent except in specific circumstances where collection, use or disclosure without consent is authorised or required by law.

Consent may be collected through written documentations (e.g., consent form, written note, registration forms, etc.) or electronically (email consent, electronic forms). In situations that consent

cannot be conveniently obtained in written form or electronically, the Church may opt to obtain verbal consent and documented provided such process is approved by the DPO.

The Church may inform the individuals that it will not be able to fulfil certain services or arrangements if they are unwilling to provide consent to the collection, use or disclosure of certain personal data.

3.3 Deemed consent

The Church may deem that an individual's consent was obtained for personal data collected prior to 2 July 2014 for the purpose of which the personal data was collected. The consent may include for the Church's usage and where applicable include disclosure.

The Church need not seek consent from staff (including volunteers and part-time workers) for purposes related to the staff's work in the Church. However, staff's consent must be obtained if such purpose is unrelated to their work. Staff are to be informed that their personal data may be disclosed to public and arrangements may be made to limit such disclosure with mutual agreement.

3.4 Consent withdrawal

Any individual may withdraw their consent to the use and disclosure of their personal data at any time by writing to the DPO, unless such personal data is necessary for the Church to fulfil its legal obligations. The Church will comply with the withdrawal request, and inform the individual if such withdrawal will affect the services and arrangements between the individual and the Church. The Church may cease such services or arrangements as a result of the withdrawal.

3.5 Notification obligation

The Church will collect personal data directly from Individuals. However, the Church may also collect individual's personal data from third parties provided the consent was obtained from the individual or required by law.

3.6 Accuracy obligation

The Church will make every reasonable effort to ensure that individuals' information it keeps are accurate and complete. When in doubt, a request may be made to the individual for a verbal or written declaration that the personal data provided is accurate and complete.

The Church relies on individuals' self-notification of any changes to their personal data that is relevant to the Church and will ensure that personal data is updated and amended when requested.

3.7 Confidentiality and data disclosure

The Church will ensure that all personal data is kept confidential and accessible only by the DPO and authorised personnel for the purposes for which the information was sought.

The Church will not disclose or transfer personal data to third parties including internal or external organisations in or outside Singapore without the written consent of the individual except what is relevant, necessary and related to achieving the intended purposes or required by law. Disclosures and transfers will be done in a manner that is secure and appropriately aligned with PDAP requirements.

4. Security and Storage

4.1 Protection obligation

The Church is to adopt security arrangement that is reasonable and appropriate to the circumstance, while 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 unauthorised persons were to obtain, modify or dispose of the personal data. Each ministry/ committee will determine such arrangement appropriate for its purposes. The DPO will review and examine such arrangements and provide necessary recommendations.

4.2 Storage of personal data

The Church will take reasonable and appropriate security measures to protect the storage of personal data, such as:

- Marking confidential on documents with personal records clearly and prominently;
- Storing hardcopies of documents with personal records in locked file cabinet systems;
- Storing electronic files that contain personal data in secured folders.
- Archived paper records and data backup files may be stored in off-site facilities or service providers provided such facilities are secured.

4.3 Protection of personal data

All personal data will be secured and protected against unauthorised access and theft.

The Church will ensure that:

- The Church's IT network that host personal data is secured and protected against unauthorised access.
- Personal computers and other computing devices that access personal data must be password protected. Passwords are managed in accordance with industry best practices.
- Personnel and other files that contain sensitive or confidential personal data are secured and only made available to staff with authorised access.
- IT service providers' services or provisions comply with security standards in line with industry practices.

In the event of a security breach, the DPO is to be notified. The DPO will investigate if such breach is a malicious act and will take appropriate action after consulting with the Pastor-in-Charge, LCEC Chairperson and Governance Chairperson.

4.4 Retention limitation obligation

The Church will retain individual's personal data only for as long as it is reasonable to fulfil the purposes for which the information was collected or as required by law. Otherwise, retention period of personal data should not exceed a period of 7 years.

The Church will ensure that the disposal of personal data is performed appropriately with little possibility to recover the information from disposal process. Such method may include shredding paper records and permanent deleting and wiping of electronic records.

5. Access and Correction Process

5.1 Access to personal data

Individuals are allowed to access to their personal data kept by the Church.

5.2 Correction of personal data

Requests for personal data correction and enquiries on data usage and disclosure should be directed to the relevant authorised staff.

Feedback and complaints are to be directed to the DPO. The Church may request for additional information from the individual to aid in the investigation.

Staff handling such requests, enquiries, feedback and complaints must verify the identity of the individual before responding.

The Staff must document such requests, enquiries, feedback and complaints and may respond via telephone call, written note or electronic mail.

Response and follow-up action must be carried out within reasonable time and documented for future reference and verification and reported to the LCEC and Governance Committee.

5.3 Openness obligation

The Church is responsible to communicate to all staff, including part-time staff and volunteers, declaring the manner that their personal data are collected, used and disclosed. The policy will be made available to staff upon request, or may be published in an appropriate manner that the Church deems fit.

The Church may make the policy available to other parties (non-staff) upon request.

6. CCTV, Video Recording and Photography

CCTV, video footage and photos may constitute personal data if an identifiable individual is captured.

- Appropriate notices are put up at the gate, church entrance, to clearly state the use and purpose of CCTV video surveillance.
- Notices are put up at church entrance, or any other prominent areas to inform visitors and volunteers that photographs and videos taken may be used by the Church for communication purpose in print or electronic media.
- For special event, it should be stated in the invitation that photographs of attendees will be taken at the function for publicity on print and electronic media. Appropriate notices should also be put up at the reception or entrance to inform the attendees on the event day.
- If photos and videos are taken out of the context of the above, the Church must obtain the individual's consent before using them.

Only authorised personnel of the Church, are allowed to access these personal data. Where in doubt, seek the advice of the DPO.

7. Policy Review and Compliance

This Personal Data Protection Policy will be maintained and updated by the DPO.

The Governance Committee is to conduct an internal audit annually to review the Policy and may use the Personal Data Protection Checklist promulgated by the Personal Data Protection Commission. After the audit, the DPO is to make the necessary enhancements and/or amendments of this Policy where applicable in consultation with the Governance Committee for final approval from LCEC.