CATHOLIC FAMILY LIFE
PERSONAL DATA PROTECTION ACT (PDPA) POLICY

1 DEFINITIONS

“CFL" or "charity” refers to Catholic Family Life – comprises Catholic Family Life Limited and CFL Lumens Trust.

“ARC” refers to the Audit and Risk Committee of CFL.

“DPO” refers to the Data Protection Officer of CFL.

“PDPA” refers to the Personal Data Protection Act.

“PDPC” refers to the Personal Data Protection Commission.

“Data Users” refers to CFL’s staff, volunteers, contractors, other third parties, subsidiaries and affiliates who generate, acquire, use, transfer, store and manage personal data and information assets.

“Data” refers to facts, figures, or other outputs from devices that are represented in a format suitable for processing by a computer.

“Information” refers to the combinations of data that provide value or inherently have value. As an example, a contact number, is generally of little value by itself. When combined with the corresponding enterprise name and product offering, the number then has significant value and can be considered an asset to the party that possesses the information.

“Information Systems” refers to IT applications, IT infrastructure and data and information assets (i.e. hardcopy and digitised data) that CFL uses, processes, and stores using those systems.

“Personal data” refers to data and/or information assets, whether true or not, about an individual who can be identified from that data, or from that data and other information to which an organisation has or is likely to have access. These data can range from names, NRIC numbers, contact numbers, addresses and images to other types of data that do not directly identify an individual on its own but form a part of an accessible record about an individual.

“Processing” refers to any operation or set of operations that are performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Data Intermediaries" refers to an organisation that processes personal data on behalf of CFL.

"Policy" refers to this Personal Data Protection Act Policy.

2.0 INTRODUCTION

The PDPA governs the collection, use, disclosure and care of individuals' personal data by organisations in a manner that recognises both the right of individuals to protect their personal data and the need of organisations to collect, use, disclose and care of personal data for purposes that a reasonable person would consider appropriate in the circumstances.

3.0 POLICY

The Policy defines the required components for CFL's personal data and information assets to be retained, taking into account their legality, value, sensitivity and criticality to the charity.

3.1 Objective

This Policy aims to ensure that all Data Users are fully aware of and comply with the PDPA requirements. This document defines the key data protection requirements. It sets forth the minimum requirements governing the collection, usage, disclosure, storage or destruction of such personal data and information assets.

3.2 Owner

The DPO will be the owner of the PDPA Policy and held accountable for the overall management and protection over the access of personal data. The DPO will act as the first point of contact for all matters related to the PDPA Policy. The Policy will have to be reviewed at least annually, or as needed.

3.3 Applicability

The Policy applies to information systems, including IT applications, IT infrastructure and data and information assets (both hardcopy and digitised data) that CFL uses, processes, and stores using those systems. Likewise, the Policy applies to the business processes and procedures of the organisation regarding personal data and information storage and retention.

3.4 Terminology and Interpretation

The following words have a specific meaning in the context of the PDPA Policy and subordinate documents.

Words	Meaning
"must" or "will"	It is mandatory to implement the action defined in the requirement.
"must not" or "will not"	The action defined in the requirement is absolutely prohibited.
"should"	It is mandatory to implement the action defined in the requirement, unless there is a business justification not to implement it, or it is currently a technology impossibility to implement it.
"should not"	The action defined in the requirement is prohibited, unless there is a business justification to allow it, or it is currently a technological impossibility to omit it.

4.0 PDPA OBLIGATIONS AND REQUIREMENTS

The PDPA requires CFL to comply with ten (10) personal data protection obligations that specify the standards to be met when processing personal data. Furthermore, the PDPA has additional requirements requiring the charity to check the Do Not Call Registry when attempting to contact (i.e. phone call, SMS, or fax) an individual for which consent has not been sought; and these obligations should be adhered to by Business Representatives, Data Custodians and Data Users when the processing of personal data and information assets as follows:

PDPA Obligation and Requirements	Description
1. Consent Obligation	The consent obligation requires CFL to: • Obtain consent to collect, use or disclose individuals' personal data; and • Allow individuals to withdraw consent Therefore: • Through the DPO, ensure that appropriate consent clauses have been drafted to support the collection, usage, disclosure or storage activity. • Collect and store the appropriate consent clauses agreed upon by the individual. • Prior to performing any activities relating to the collection, usage, disclosure or storage of personal data, appropriate consent must be sought from the individual. • There is a need to cease collecting, using, or disclosing personal data when the individual has withdrawn his/her consent.

	• Work with the DPO to ensure that in the course of providing a service or product, an individual must not be required to consent to the collection, use, disclosure or storage of his / her personal data beyond what is reasonable to provide the product or service. For example: ● Obtain consent for marketing purposes through a checkbox. ● Contact the individual and confirm the consent in writing where the customer has provided verbal consent. Charities should minimally state and comply with the purpose for collecting, using and disclosing personal data. Consent should be requested and provided to individuals. There are five types of consent for this purpose: Expressed Consent, Deemed Consent, Withdrawal Consent, Dynamic Consent and Invalid Consent. Note: The PDPA (Amendment) Act 2020, effective 1 February 2021, introduced two additional lawful bases under the Deemed Consent framework. (1) Deemed Consent by Contractual Necessity (s.15(3)–(8)): Where an individual provides personal data to CFL in connection with a contract, CFL may share that data with third parties to the extent reasonably necessary to fulfil that contract, without seeking fresh consent. CFL must document the necessity analysis and check that such disclosure is not restricted by the terms of the underlying agreement. (2) Deemed Consent by Notification (s.15A): CFL may use or disclose personal data for a new purpose without express consent, provided CFL first conducts and documents a written assessment that the use is not likely to have an adverse effect on the individual, gives the individual advance notice of the intended use and a reasonable opt-out period, and does not proceed until the opt-out window has closed. This basis cannot be used for direct marketing purposes.
2. Purpose Limitation Obligation	The purpose limitation obligation requires CFL to: ● Not make customers consent to the collection, use, disclosure, or storage of their personal data beyond what is reasonable to provide the product or service; and ● Collect, use or disclose personal data only for the purposes for which consent was obtained. Therefore, it is required that the collection, usage, disclosure or storage of personal data is based on the reasonable purposes for which an individual has given his/her consent. For example:

	• Stating that personal details are required to provide the stated services. • Stating that personal data might be transferred to third parties in the event of any re-organisation, merger, sale, joint venture, transfer, or deposition of all or any portions of the operation.
3. Notification Obligation	The notification obligation requires CFL to notify individuals of the purposes for collecting, using, disclosing, or storing their personal data. Therefore: • The Policy Owner must be informed of new collection, usage, disclosure or storage activities relating to personal data to align processes to meet PDPA requirements. • Individuals must be notified of the purposes for which personal data will need to be collected, used, disclosed or stored before or during the collection of the consent. For example: • Notifying individuals through web forms. • Notifying individuals through order forms

4. Access and Correction and Obligation	The access and correction obligation require CFL to:
	• Upon request, provide individuals with their personal data and the ways in which their personal data were collected, used or disclosed in the past year; and
	• Correct any error or omission in individuals' personal data upon their request.
	
	Therefore:
	• Upon request by an individual, inform and work with the ARC to:
	  ○ Disclose the personal data declared to CFL; and
	  ○ Disclose any usage of his/her personal data on activities that had occurred in the past year.
	• Upon request by the individual, correct any error or omission in an individual's personal data.
	• To comply with PDPA requirements, work with the DPO to ensure that all access and correction requests are provided within 30 calendar days of receiving the request.
	• Where there might be a perceived considerable effort involved in fulfilling the access request, work with the ARC in estimating the cost involved.

5. Accuracy	The accuracy obligation requires CFL to make a reasonable effort to ensure that the personal data collected is accurate and complete.

	Therefore, there is a need to conduct appropriate checks before collecting, using, disclosing, or storing to ensure that personal data collected or provided is reasonably accurate and complete.
6. Protection Obligation	The protection obligation requires CFL to put in place reasonable security arrangements to protect personal data from unauthorised access, collection, use, disclosure, storage and similar risks. Therefore: • Adherence to the Data Classification Policy and Data Access Management Policy is necessary to ensure that personal data is appropriately classified with appropriate data access management controls and standards. • Data Custodians should refer to the NE Digital Cybersecurity Policy to ensure that corresponding controls related to the Data Classifications are applied consistently. In addition to technical and administrative controls, CFL must implement physical security measures including: (a) storing hardcopy personal data in locked filing cabinets within access-controlled areas; (b) applying a clean-desk policy to prevent unauthorised viewing of personal data; (c) ensuring documents containing personal data are shredded (cross-cut, meeting at minimum DIN 66399 Level P-4) before disposal and are never placed unshredded in general waste bins; (d) maintaining visitor access logs for areas where personal data is stored or processed; (e) ensuring devices and storage media containing personal data are securely wiped or physically destroyed before disposal or reuse; and (f) restricting physical access to server rooms and data processing areas on a need-to-know basis. The standard of protection must be commensurate with the sensitivity and volume of the data held. Sensitive categories of data (including health, financial, NRIC, and children's data) require higher security controls.
7. Retention Limitation Obligation	The retention limitation obligation requires CFL to cease retention or anonymise personal data when it is no longer necessary for any business or legal purposes. Therefore: • There is a need to set appropriate retention limitations on personal data based on the limits defined in the Data Retention Policy to comply with PDPA requirements. • Cease retention of personal data or remove the personal data through means of anonymisation or pseudonymisation defined in

	the Data Retention Policy when these personal data are no longer required.
8. Transfer Limitation Obligation	The transfer limitation obligation requires CFL to ensure that the standard of protection accorded to personal data is comparable to the PDPA when it is transferred overseas. Therefore: • It is expected that personal data should not be transferred to another country or entity unless explicit approval has been sought and received from the ARC, Data Custodian, and/or Policy Owner. • Work with the ARC, Data Custodian and/or Policy Owner to ensure that an appropriate Data Processing Agreement has been put in place before transferring Personal Data to another country or entity. This will enhance the standard of protection over personal data to be comparable to PDPA requirements. • Adhere to the Data Access Management Policy and ensure that personal data is not shared with unauthorised individuals. All Data Processing Agreements (DPAs) with vendors or data intermediaries who process personal data on CFL's behalf must, at minimum, include clauses covering: (a) restriction of use to the authorised purpose only; (b) prescribed technical and organisational security measures; (c) prohibition on sub-contracting without CFL's prior written approval; (d) an obligation to promptly report any suspected data breach or security incident to CFL; (e) CFL's right to audit the vendor's data protection practices; and (f) return or irreversible destruction of all personal data upon termination of the engagement. Note that under s.4(3) PDPA, CFL remains fully liable for any breach by a data intermediary acting on its behalf. Vendor DPAs must be reviewed at each contract renewal or where there is a material change in the vendor's data processing activities.
9. Data Breach Notification Obligation	The data breach notification obligation requires CFL to assess whether a data breach is reportable, and, when necessary, perform the relevant reporting. A breach is notifiable if it results in, or is likely to result in, significant harm to affected individuals (e.g. exposure of financial, medical, or NRIC data combined with other identifiers), or if it affects 500 or more individuals. Upon assessing a breach as notifiable, CFL must notify the PDPC no later than 3 calendar days after the assessment is made. Affected individuals must also be notified where there is a risk of significant harm to them, unless effective remedial action (such as encryption) has already been taken. CFL must maintain a written Incident Response Plan that covers: (a) steps for containing

	and assessing a suspected breach; (b) escalation to the DPO within 24 hours of discovery; (c) breach assessment and documentation; (d) PDPC notification via the online portal within 3 calendar days of a notifiable assessment; and (e) notification to affected individuals where required. All breach incidents, whether notifiable or not, must be documented and retained for audit purposes.
10.Accountability Obligation	The accountability obligation requires CFL to be accountable for the protection of personal data. Therefore: I. Whenever necessary, work with the DPO to update the personal data protection notification. II. Be accountable for collecting, using, disclosing or storing personal data and ensure that they comply with the PDPA Obligations. III. Be accountable towards the management and protection of personal data within CFL. IV. Be accountable and report personal data breaches to the DPO, Data Custodian and/or Policy Owner. V. Work with the DPO, Data Custodian, and/or Policy Owner to ensure appropriate safeguards are in place to protect personal data. Policies for data protection/privacy should be developed and implemented. These policies should be communicated and practised by their staff. Charities may need to consider implementing appropriate governance controls to manage data and their third parties. CFL should conduct a Data Protection Impact Assessment (DPIA) before implementing any new information system, process, or product that involves the collection or use of personal data, particularly where sensitive data is involved, where large volumes of data will be processed, or where the system or product is likely to be accessed by children. A DPIA should identify privacy risks, assess their likelihood and impact, and document mitigation measures. DPIA records must be retained and reviewed when the underlying system or process changes materially.
11.Data Portability	The data portability obligation requires CFL to transmit an individual's personal data in a readable form when requested by the individual. Therefore:

	I. Ensure secure methods are used when transmitting data to another organisation or individual. II. Work with the DPO/Policy Owner to ensure that a process has been put in place to respond to data porting requests within 20 working days.
12. Do Not Call (DNC) Registry	The DNC provisions prohibit organisations from sending certain marketing messages to Singapore telephone numbers, including mobile, fixed-line, residential and business numbers registered with the DNC Registry. Therefore, there will be a need to work with the DPO to check on the DNC Registry when contacting an individual via a phone call, SMS, or fax, for which appropriate consent has not been obtained. Staff of CFL can contact the individual without the need to check the DNC Registry should prior consent be given. Consent is also not necessary should there be a need to respond to an emergency that threatens the life, health or safety of the individual or another individual, or if the personal data is publicly available.

Corresponding guidelines to the above obligations can be found in the advisory guidelines released by the Personal Data Protection Commission at - https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Advisory-Guidelines-on-Key-Concepts-in-the-PDPA-1-Feb-2021.pdf?la=en

It is a requirement under the PDPA for CFL to comply with the above ten (10) obligations and two (2) requirements on Data Portability and the Do Not Call Registry, in addition to registering at least a DPO representative for each of the business entity/vehicle that operates in Singapore.

5.0 CATEGORIES OF PERSONAL DATA

CFL should define the type of personal data that they hold. This will allow the readers of the PDPA Policy to be aware of the defined categories of Personal Data. The following categories are examples of personal data that CFL may hold:

- Donors

- Employees and Volunteers:
  - Permanent staff
  - Temporary and contract staff
  - Resigned staff

- Volunteers

- Job Applicants:
  - New job applicants
  - Prospective job applicants
  - Rejected job applicants

- Others:
  - Employees of vendors and suppliers
  - Visitors to CFL's premises
  - Service recipients and beneficiaries (individuals and families receiving CFL's programmes, counselling, or support services, including minors where applicable)

6.0 PDPA GOVERNANCE

To ensure continuous enhancements of business processes to comply with existing and/or new PDPA requirements, the DPO will work on the following:

- To receive and respond to complaints that may arise concerning the application of the PDPA;
- To receive and respond to requests for access and correction to information;
- To work with the DPO regarding the governance of personal data;
- To work with legal to comply with PDPA legislation requirements;
- To communicate, both internally and externally, on CFL's policies and practices, as well as other PDPA-related matters; and
- To design and conduct awareness training on personal data protection for all new and existing employees, and external parties like temporary/contract staff and volunteers via various training platforms and methods.

7.0 GENERAL OFFENCES AND PENALTIES OF PDPA

The PDPC is the designated authority responsible for overseeing the PDPA. The PDPC may provide the following directions when CFL has been deemed to be found non-compliant with the PDPA provisions:

7.1 Sensitive Categories of Personal Data

Although the PDPA does not prescribe a statutory list of sensitive categories, the PDPC treats certain data types as warranting higher protection. CFL must apply enhanced safeguards to: (a) health and medical information; (b) financial and insurance data; (c) NRIC and passport numbers; (d) religious affiliation and beliefs; (e) personal data of minors (see Section 7.2); and (f) any data whose exposure is deemed to cause significant harm under the Data Breach Regulations (S 64/2021). Enhanced safeguards include strict need-to-know access controls, encryption in transit and at rest, and mandatory review before any secondary use or disclosure. NRIC numbers must

not be used as passwords, PINs, or authentication credentials in any CFL system, in accordance with the PDPC–CSA joint advisory of 26 June 2025.

7.2 Children's Personal Data

The PDPC's Advisory Guidelines on Children's Personal Data (March 2024) treat children's data as a sensitive category requiring higher protection. A "child" is any individual under 18 years of age. As CFL serves families and may hold data of minors through its programmes, CFL must: (a) obtain parental or guardian consent for collection and use of personal data of children under 13; (b) for children aged 13 to 17, ensure consent is genuinely informed, using clear and simple language; (c) collect only the minimum data necessary for the specific programme; (d) apply heightened access controls to all data relating to children; (e) conduct a DPIA before introducing any programme or system that collects children's data; and (f) not use children's data for profiling or marketing without explicit parental consent.

7.3 Roles and Responsibilities

(a) Data Protection Officer (DPO): Owns and maintains this Policy; oversees breach assessment and PDPC notification; handles access and correction requests; manages vendor DPAs; and coordinates staff training. The DPO must be registered with the PDPC. A designated backup contact must be named in the DPO's absence. (b) Audit and Risk Committee (ARC): Provides governance oversight; approves cross-border transfers; reviews the annual PDPA compliance report; and considers DPIAs for high-risk activities. (c) Data Custodians: Department heads and programme managers are accountable for data under their remit and must report any suspected breach to the DPO promptly. (d) Data Users: All staff, volunteers, and contractors who access personal data must comply with this Policy and complete PDPA training upon onboarding and at least annually thereafter.

7.4 Consequences of Non-Compliance

Any Data User who breaches this Policy may be subject to disciplinary action by CFL, up to and including termination of employment or engagement. Where a breach involves deliberate or negligent misuse of personal data, the matter may be referred to the relevant authorities. Staff must not conceal or fail to report a suspected breach. Retaliation against any individual who reports a breach in good faith is prohibited.

7.5 Policy Version Control and Review

This Policy must be reviewed by the DPO at least annually, or earlier following a material change in CFL's operations, a significant data incident, or an update to PDPA legislation or PDPC guidelines. Each version must carry a version number and effective date. A summary of changes must be recorded. All updates must be communicated to Data Users and evidence of training acknowledgement retained. A version history table (Version | Effective Date | Author | Summary of Changes) must be maintained and appended to this Policy.

8.0 GENERAL OFFENCES AND PENALTIES OF PDPA

- To stop collecting, using or disclosing personal data in contravention of the PDPA;
- To destroy personal data collected in contravention of the PDPA;
- To comply with any direction of the PDPC; and
- To pay a financial penalty of such amount not exceeding 10 percent of annual gross turnover or $1 million (whichever is larger) as the PDPC deems fit.

The Commissioner's decisions are published on the PDPC's website for public viewing. Therefore, Data Users should ensure that the usage of personal data should comply with the PDPA obligations to avoid causing any reputational damage to the enterprise.

Last updated: 1 June 2026