KOINONIA
INCLUSION
NETWORK

Personal Data Protection Policy

Doc. ID:	PDPP-2023v1
Document Name:	Personal Data Protection Policy
Document Version:	1.0
Document Effective Date:	10 June 2023
Document Ownership:	Data Protection Officer

Version History

Name / Ministry	Changes Made	Approved by	Version No.	Date
DPO/Admin	Initial release	MC	1.0	10 June 2023
DPO/Admin	Changed “Management Committee” to “Board of Management’ and “Sub-Committee” to ‘Committee’	As per new Constitution	1.1	7 September 2023

Contents

1 INTRODUCTION

1.1 Purpose of Policy

This Policy is prepared by Koinonia Inclusion Network (KIN) and is approved by the KIN Board of Management.

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

1.2 Policy Statement

Under the PDPA, KIN will inform the individual of the purposes for which his/her personal data will be collected, used or disclosed on or before such collection 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.

KIN 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 KIN's endeavour to:

i. Take all necessary efforts to comply with the PDPA requirements;
ii. Ensure that individuals' personal data are not misused;
iii. Help, train and support staff and volunteers who handle personal data to understand the requirements of the Policy and to act appropriately;
iv. Respond to any legitimate enquiries regarding usage, storage and accuracy of 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 KIN 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

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

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

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

Use – The term 'use' refers to any act or set of acts by which KIN 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 KIN 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 KIN to ensure and demonstrate compliance with the PDPA through proper management and protection of personal data.

KIN is answerable to regulatory authorities and individuals who entrust KIN with personal data, and will implement the necessary policies and procedures to fulfil its PDPA obligations.

The KIN Personal Data Protection Policy summary is available on the KIN website at https://kin.org.sg/privacy-policy/.

3.1 Data Protection Officer

The KIN-appointed Data Protection Officer ("DPO") is accountable to the KIN Executive Director and the KIN Board of Management. The DPO will work with all concerned parties to ensure compliance of the PDPA.

The DPO's duty is to oversee data protection responsibilities and ensure compliance with the PDPA.

3.2 Responsibilities of the DPO

The responsibilities of the DPO include, but are not limited to:

- Ensuring compliance with PDPA when developing and implementing policies and processes for handling personal data;
- Fostering a data protection culture among employees and communicating personal data protection policies to stakeholders;
- Managing personal data protection-related queries and complaints;
- Alerting management to any risks that might arise with regard to personal data; and
- Liaising with the PDPC on data protection matters, if necessary.

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

Koinonia Inclusion Network
133 Fidelio Street
Singapore 458518

or via email to dpo@kin.org.sg

4 COLLECTION OF PERSONAL DATA

4.1 Notification Obligation

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

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

KIN will inform 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 KIN 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.

The means of collection include but are not limited to:

a. Application forms or personal data submitted by an individual to KIN relevant to all events and activities organized or managed by KIN;
b. Where an individual contacts the staff or representatives of KIN to make

enquiries in relation to consultation, sales etc., whether such contact is by email, voice calls or any other medium;

c. Where an individual makes a donation to KIN;
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 KIN events, activities, programmes or courses.

KIN 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. This may include the following purposes within the organisation's operations:

a. Pledges
b. Society Membership
c. KIN activities / courses / events
d. Pre-employment application / employee appointment

4.2 Consent Obligation

KIN 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.

KIN 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 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, although he/she has not expressly stated his consent in written or verbal form.

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

KIN need not seek consent from employees (including volunteers and part-time workers) for purposes related to their work in KIN. However, an 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

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.

KIN 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 KIN to fulfil its legal obligations.

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

4.3 Purpose Limitation Obligation

KIN 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

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

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

5.2 Protection Obligation

KIN 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 KIN 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 KIN 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

KIN will retain the individual'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.

KIN will review the personal data that they hold on a regular basis to determine if that personal data is still required.

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

KIN will use appropriate security measures when destroying personal data, including shredding paper records and permanently deleting electronic records.

5.4 Transfer Limitation Obligation

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

a. National Council of Churches in Singapore (NCCS), 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 KIN;
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.

KIN 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.

KIN 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 KIN 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 KIN 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 letter 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 KIN in writing to the DPO (see 3.2).

6.2 Data Breach Notification Obligation

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. KIN will put in place measures which monitor and take pre-emptive actions to prepare for data breaches.

KIN will notify the Personal Data Protection Council (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.

KIN 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 KIN's Audit Committee to review and monitor compliance to this Policy.

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