Data Governance Policy

Drafted By	Jessica Macpherson	Reviewed By	Matthew Craven, HWL Ebsworth
Version	1	Approved By	Board
Category	Governance	Approved Date	01 April 2019
Type	Risk Management	Review Date	31 March 2021

Introduction

St Kilda Mums (also trading as Geelong Mums and Eureka Mums) (the **Organisation**) is provided with data from a number of different sources, including staff, volunteers, donors, social services, beneficiaries, suppliers and members of the public.

Data is critical to the effective operation of St Kilda Mums. It allows St Kilda Mums to operate day-to-day, monitor its performance as well as identify where it could expand or improve upon its services.

A breach of the Privacy Act or disclosure of confidential information could result in substantial penalties and damage to our reputation. The costs of proper management of data records are negligible compared to the benefit of reducing these risks.

This Policy establishes a governance framework that applies to data so that risks are managed and the security and integrity of data is maintained.

Scope

This Policy applies to all our officers (paid employees and volunteer), and any consultants or contractors we may engage to support us. It is the responsibility of all Personnel and Contractors to have a full understanding of this Policy.

Contents

Purpose

The purpose of this Policy is to:

- set out the principles that the Organisation will adhere to in the oversight, management and use of data;
- define the roles and responsibilities for data governance and usage and establish clear lines of accountability;
- develop measures for effective data management and protection, including measures which govern how data is accessed, retrieved, reported, managed, stored and destroyed; and
- Ensure that The Organisation complies with applicable laws, regulations, and standards.

This Policy supplements the Privacy Policy. For information on what personal information the Organisation collects and uses, how that information is stored and handled, how individuals can request access to and correction of their personal information, and The Organisation's privacy complaints process please refer to the Privacy Policy.

Definitions

Access means the right to read, copy or use data.

Contractors means consultants or contractors the Organisation engage from time to time, and their officers, employees and agents who receive or have access to data held by the Organisation.

Data refers to information in the Organisation's resources and records, which fall within four broad categories:

- Public data: data that is openly available to the general public.
- Internal data: data used by the Organisation to administer its services and not for external distribution unless otherwise authorised, such as information about Personnel.
- Protected data: data that is only available to Personnel with the required access in order to perform their assigned duties or Contractors that require the Data to perform obligations to the Organisation. Within this category of data is personal information, please refer to the Privacy Policy for further details on how the Organisation treats personal information.
- Restricted data: data that is of a sensitive or confidential nature and is restricted from general distribution. This data will only be distributed if required by law. Within this category of data is sensitive information please refer to the Privacy Policy for further details on how the Organisation treats sensitive information.

For the avoidance of doubt, all data collected by the Organisation is (as between the Organisation and its Personnel and Contractors) owned and controlled by the Organisation. See the Privacy Policy for further.

Data Governance Hierarchy outlines the access rights, roles and responsibilities of The Organisation Personnel and Contractors in relation to the management and protection of data.

Data Governance Measures set out how the Organisation will manage and use its data.

Paper Records means any information, including personal information that is written, printed, inscribed or otherwise recorded on paper or any substance with a similar function.

Personal information means any information or an opinion (whether true or not and whether recorded in a material form or not) about an individual who is identified or reasonably identifiable from the information;

Personnel means officers, employees and volunteers of the Organisation, whether paid or not.

Privacy Act means the Privacy Act 1988 (Cth).

Privacy Policy means the the Organisation's Privacy Policy.

Quality Assurance means the process of ensuring the accuracy and currency of data at its creation and over its lifecycle.

sensitive information is a subset of personal information and means (without limitation) information about an individual's race, political opinions, religious beliefs, philosophical beliefs, membership of a trade union, sexual preference, criminal record, or health, genetic or biometric information, including "sensitive information" as defined in the Privacy Act.

St Kilda Mums Inc, **we**, **us** and 'our' mean the organisation carrying on business under the name St Kilda Mums, including Geelong Mums and Eureka Mums;

Principles

The Organisation will adhere to the following principles in overseeing, managing and using data.

1. Collection

When receiving personal information, such as names, emails, contact numbers and address details, and any other information relating to identified individuals the Organisation is required to will take reasonable steps to ensure the individual is aware of :

- The Organisation name and contact details;
- our purposes for collecting the personal information;
- who we ordinarily disclose that kind of personal information to;
- that our Privacy Policy contains information about how the individual may request access to or correction of personal information we hold about them, how they can complain about our privacy procedures and how we will deal with such complaints;
- that we use service providers located overseas (including in the United States) to store and process personal information;
- the main consequences (if any) if the individual does not provide the personal information requested; and
- details of any law or court order that requires or authorises us to collect the personal information (if applicable).

Where possible, the Organisation should collect personal information directly from the individual concerned.

In cases where it is impractical to collect the relevant information from the individual directly and we need to collect it from other sources, St Kilda must take reasonable steps to let the individual know that we have collected this information and the circumstances this was done (in addition to the details listed above), unless they are already aware of this.

2. Consent

Where practicable to do so, when collecting sensitive information or if the Organisation intends to use or disclose personal information in a manner that the relevant individual would not reasonably expect, then in addition to providing the information outlined in section 1 above, the Organisation should also obtain the informed consent of the individual to such use or disclosure.

Express consent will be sought in a number of ways—including filling in a form, ticking a box on the the Organisation's website, over the phone, or face-to-face.

The Organisation will keep a record of all instances where consent is given and how it was given.

In limited circumstances, consent may be inferred. In particular, consent to contact someone may be inferred if their contact details are published and are accessible to the general public, our reason for wanting to contact the individual is related to the reason the individual published their details and there is no statement accompanying those contact details making it explicit that contact from a not-for-profit organisation is not wanted.

3. Security

The Organisation will take reasonable steps to protect the Data we hold or control from misuse, interference, loss, and unauthorised access, modification or disclosure. This includes:

- using secure devices and servers;
- imposing security restrictions on computers, including requirements for complex passwords where Protected and Restricted Data may be accessible;
- utilising two-factor authentication protocols where available;
- implementing encryption mechanisms to keep Protected and Restricted Data secure, both while in transit and at rest;
- adopting protection measures on our websites, including encryption and firewalls;
- installing and regularly updating software, including anti-virus software on all computers and devices;
- maintaining controlled access to the Organisation's premises; and
- securely storing any Paper Records.

Protected and Restricted Data (including personal information and sensitive information) may only be collected, handled, used, accessed and disclosed by Personnel and Contractors pursuant to the Data Governance Measures detailed further below, and only if and to the extent such Personnel or Contractors need access to that information to perform their obligations to the Organisation.

Personnel and Contractors must only access and use Internal, Restricted and Protected Data if and to the extent necessary to perform their role.

The security settings for access to Internal, Restricted and Protected Data must be set in a manner which minimises the risk of inadvertent or deliberate unauthorised access by Personnel or Contractors that do not require access to perform their roles.

Access rights should be periodically reviewed to ensure they are up to date (for example, to remove access to Personnel or Contractors that have changed role or ceased to work for the Organisation).

All Paper Records and data storage devices containing Internal, Restricted and Protected Data must be stored in locked secure cabinets at the Organisation premises or at third party premises approved by the Chief Executive Officer.

All Internal, Restricted and Protected Data must be stored on approved and secure data storage devices (such as external hard drives, discs, USB flash drives, etc.), must be password protected and securely encrypted unless otherwise approved by the IT manager.

Our security arrangements are supported by related policies and operational processes aimed at minimising the risk of a data breach.

4. Clean Desk

Paper Records, especially those containing Internal, Protected and Restricted Data (such as confidential information, personal information and sensitive information) must be securely stored when not in use and must not be left unattended on desks or in a position where they may be accessed by anyone who does not have appropriate rights or a legitimate need to access them.

5. Shred All

All Paper Records containing Protected and Restricted Data (including personal information and sensitive information) must be transferred to electronic format as soon as practicable and the Paper Records destroyed, unless they are legally required to be retained as Paper Records for a period of time.

Personnel must ensure the destruction of Paper Records is done in a secure and confidential manner. This should generally be done by shredding the Paper Records on-site either by Personnel or by the Organisation's contracted shredding contractor. Shredding is a means of destroying Paper Records by mechanical cutting into strips or particles that results in all information being incapable of reconstruction.

6. Quality and Integrity

At each stage of the data lifecycle, from collection to use, disclosure, accessibility, storage and disposal, the Organisation will put in place processes to ensure the quality of the data is maintained.

For example, the Organisation will aim to reduce its reliance on manual inputting processes so as to avoid error. The Organisation aims to follow the data minimisation principle so as to not collect and use data that is not required for the organisation purposes.

When working with data records, the Organisation will ensure that personal information and privacy preferences changes are traceable.

If Personnel have contact with individuals for whom the Organisation holds personal information and the Organisation has not had contact with those individuals for some time, Personnel need to check that our records relating to individuals contact details are still correct and up to date (and modify them if they are not).

The Organisation will regularly audit the Data we hold to determine whether the personal information about an individual is still needed for the purpose it was collected or for any other purpose (including any record-keeping requirements required by law). Where personal information is no longer needed or required to be kept by law, the Organisation will either destroy it or permanently de identify it.

In the instance of a data breach or privacy incident, the Organisation has practice measures in place to contain, assess, and mitigate the breach or incident. See our Data Breach Incident Plan for further details.

7. Openness

Subject to complying with the other principles and the procedural requirements related to this Policy, the Organisation may use aggregated / anonymised data to:

- provide an overview to partners, sponsors, donors, government departments and the general public on how it uses their donations as well as the scale and scope of the Organisation' sservices; and

- assist its sister organisations that provide similar services to that of the Organisation.

The Organisation will permit an individual to access and correct any Data (that is personal information of the individual) that the Organisation holds where required by law and otherwise in accordance with the Organisation's Privacy Policy.

Data Governance Hierarchy

The roles and responsibilities for data are set out below:

The Board is responsible for:

- approving the Data Governance Policy; and

- approving the necessary resources required to establish, implement, operate, review, maintain and improve Data Governance.

Chief Executive Officer is responsible for:

- managing the overall establishment, implementation, maintenance, and continual improvement of Data Governance Measures;
- overseeing the capture, maintenance and use of data under the Data Governance Measures;
- assisting Personnel with developing, maintaining, distributing and securing data;
- ensuring the data complies with Quality Assurance, if collecting it; and
- Ensuring that Personnel are trained in, and at all times comply with, this Policy including the Data Governance Measures.

Managers are responsible for:

- assisting the Chief Executive Officer with any of their responsibilities as set out in this Policy; and
- overseeing compliance with data operating procedures that are made pursuant to this Policy and the Data Governance Measures.

Personnel of the Organisation are responsible for:

- recording, accessing, amending, deleting, extracting and analysing data as needed to exercise their functions;
- ensuring the Quality, Integrity and Security of data at all times; and
- only handling Data in a manner consistent with the terms of this Policy.

Data Governance Measures

Data will be extracted, manipulated, analysed and reported by the Organisation to exercise its functions in line with its vision and values.

Personal use of Internal, Restricted and Protected Data, including data that is derived from this data, is prohibited.

Where appropriate, before any data (other than publicly available data) is used or shared outside the Organisation, the Chief Executive Officer will verify that the quality, integrity and security of data will not be compromised and will ensure that the data is appropriately aggregated and de-identified.

The Organisation needs to treat any potentially re-identifiable Data confidentially and in accordance with any legal obligations that apply to that Data (such as the Privacy Act). Accordingly, consideration needs to be given as to whether the aggregated Data that is proposed to be released could be combined with other datasets (such as those publicly available or in the possession of the likely recipients of the aggregated Data) which would allow any individuals in the aggregated Data to be identified. Specialist data science expertise can be sought to assess the re-identification risk, if required.

All data will be stored in an electronic format giving preference to cloud based over local storage. Data provided in the form of Paper Records will be transferred to electronic format and Paper Records will be shredded in accordance with the Shred All (unless there is a legal obligation to retain the Data as a Paper Record.

All data except public data will be kept in a secure location and protected by appropriate electronic safeguards and/or physical access controls that restrict access only to authorised user(s).

Appropriate data security measures must be adhered to at all times to assure the safety, quality and integrity of data.

Any Contractors that the Organisation engages and who will have access to material Data must be required to keep any Data confidential, and required to either comply with this Policy or otherwise be subject to contractual obligations in favour of the Organisation that are consistent with the requirements of this Policy. Periodic reviews should be undertaken to review the Contractor's compliance with these requirements.

Review

This policy will be reviewed and updated every two years or sooner if required. It will be readily accessed by all staff via the People & Policy App on Salesforce.

This policy will be published on the St Kilda Mums website.

Any questions in relation to this Data Governance Policy, please contact the CEO.

Policy Implementation Documents

The following documents are to be used in conjunction with this policy:

- Privacy Policy
- Data Breach Incident Response Plan