Data Handling Policy

**Umina SLSC**

**September 14, 2023**

Contents Page

[1 Purpose 1](#_Toc144209647)

[2 Scope 1](#_Toc144209648)

[3 Data Management Guiding Principles 1](#_Toc144209649)

[4 Data Handling 2](#_Toc144209650)

[5 Data Classification 2](#_Toc144209651)

[5.1 Public Information 2](#_Toc144209652)

[5.2 Personal Information 3](#_Toc144209653)

[5.3 Sensitive Information 3](#_Toc144209654)

[6 Data Use 3](#_Toc144209655)

[7 Data Retention & Disposal 3](#_Toc144209656)

[8 Enforcement 4](#_Toc144209657)

[9 Revisions 4](#_Toc144209658)

[10 Document History 4](#_Toc144209659)

[11 Document Control Log 4](#_Toc144209660)

# Purpose

This Policy identifies what is required to ensure appropriate governance, assurance, and integrity for handling data. The principles laid out in this Policy are designed to provide a consistent assurance to all parties involved that the integrity of the data is always maintained, from its collection to eventual disposal or archiving.

This assurance is crucial in an age where data breaches and mismanagement can have significant, far-reaching consequences both legally and reputationally. This comprehensive approach reinforces the company's commitment to data integrity, security, and privacy.

# Scope

This policy encompasses all data that Umina SLSC interacts with, irrespective of its nature or origin. Whether it’s data related to members, family groups, employees, partners, or internal operations, all fall under the purview of this policy. This broad applicability ensures a consistent and robust approach to data management across all departments, teams, and initiatives within Umina SLSC.

Every individual associated with Umina SLSC, be it volunteers, members, permanent staff, temporary workers, or third-party vendors, is expected to be familiar with and adhere to this policy when handling or interacting with data affiliated with Umina SLSC.

This document forms part of the Umina SLSC Information Security Policy, and any terms or definitions from that document apply here.

# Data Management Guiding Principles

The following are guiding principles for ethical data and information management:

* Only collect the minimum amount of data/information you need to meet your purposes
* You must be able to clearly articulate your primary and secondary purpose for collecting data
* Private and personal information should be only kept for an agreed timeframe
* You must receive and record consent from someone when they give you personal or private information
* The consent should detail how the information will be used and for what specific purpose
* You must disclose if you plan to share personal or private information with external organisations
* Where possible, and especially for reporting purposes, personal information should be deidentified
* Health and medical-related information and information on minors should be very carefully scrutinised as to how it is being captured, stored and used
* Have a published, open and transparent privacy policy (notionally the [SLSA privacy policy](https://sls.com.au/privacy-policy/))
* Appoint a “Privacy Officer” who is responsible for addressing all privacy-related matters
* Do not accept unsolicited personal or private information
* Consider if third-party vendors, suppliers, contractors, etc., meet privacy policy requirements
* Keep private and personal information secure, including audit logging and being able to provide a trail of who accessed personal or confidential information
* Provide a mechanism whereby people can request whatever private or personal information you have gathered on their person and allow them to correct it if they need to
* When collecting data from SLSA systems, such as Surfguard, you must comply with the [SLSA Terms of Use](https://sls.com.au/terms-of-use/). Particularly Point 5 – You will not knowingly extract data from IT Systems and use that data in a way that could cause misuse, loss, unauthorised access, modification or disclosure. This includes storage of extracted data on external portable devices such as a USB storage device or on any online storage facility including but not limited to services such as Dropbox, Microsoft OneDrive or Google Drive. You must not also transmit any data via email or any other unencrypted transfer method;

# Data Handling

All data handled within the organisation must be treated according to its data classification as outlined below, and necessary precautions are to be taken to ensure that Public, Personal and Sensitive data is appropriately managed according to this policy to ensure it doesn’t leave Umina SLSC with a liability due to not having the necessary authorisation.

The recording of member data is the responsibility of Surf Life Saving Australia at a National level. However, it becomes the responsibility of Umina SLSC when the member data is downloaded and modified by an employee or volunteer using access granted by Umina SLSC.

# Data Classification

Data is classified into one of the following three categories:

## Public Information

This covers publicly available information and does not fall into the definition of personal or sensitive information. This can include published company information such as press releases, marketing materials and other information posted on websites or in the media. Public Information can sometimes be combined with Personal or Sensitive Information and should, therefore, be treated as such to safeguard all data.

## Personal Information

Personal information is information or an opinion about an identified or reasonably identifiable individual. This might include a person’s name and address, photos, videos and even information about what an individual likes, their opinions and where they work.

## Sensitive Information

Sensitive information is the most critical data classification for Umina SLSC’s data. It includes information or an opinion about an individual’s racial or ethnic origin, political opinions, religious or philosophical beliefs, sexual orientation, medical records, criminal record, financial information, bank account details, health information and some aspects of genetic and biometric information.

# Data Use

Data is only to be used in the manner agreed to and authorised by Umina SLSC.

* Fair data use pertains to the collection, handling, and dissemination of data, ensuring that the rights of individuals are protected, and the intentions behind data usage are transparent and justifiable
* This means obtaining informed consent from individuals when collecting their data and being transparent about its use
* Fair data use is not just a legal obligation but establishes trust between data subjects and data handlers
* Any use of data other than that agreed to by Umina SLSC, such as for personal or other use, may result in disciplinary action being taken

# Data Retention & Disposal

The organisation must manage the data lifecycle effectively to guarantee that Personal and Sensitive data remains secure and doesn't exit Umina SLSC’s systems. Once the data is no longer needed, it must be promptly deleted.

* Member data should be securely retained throughout its lifecycle and be easily accessible to guarantee timely service delivery
* Every piece of data collected should have a clear purpose. Consent must be documented when Personal Information is gathered, and a date for data disposal should be set
* Data may only be stored on systems that provide enterprise-grade encryption
* Access to data stores is to be access controlled
* Removable media such as USB drives should not be used to store Personally Identifiable or Sensitive Data
* When a member’s membership ends, all data collected by the member must be permanently deleted from all systems Umina SLSC provided to the member, volunteer or employee

# Enforcement

Each staff member or volunteer is expected to comply with this policy. If there is any failure to observe the procedure, disciplinary measures may be taken. The steps which may be taken will vary according to the breach and the circumstances of the violation. However, the right is reserved to terminate the membership or employment of any staff member or volunteer who breaches this policy via the [SLSA Complaints Resolution Policy](https://www.surflifesaving.com.au/wp-content/uploads/sites/2/2021/11/Policy-6.06-Complaints-Resolution-2022.pdf).

# Revisions

This policy document will be periodically revised as risks, systems, and business practices change.

# Document History

|  |  |
| --- | --- |
| Title | Data Handling Policy |
| Classification | Internal |
| Creation Date | September 14, 2023 |
| Last Review Date | September 14, 2023 |
| Author | Matthew Ingersole |
| Owner | Chief Information Officer |
| Document Number | P-03 |

# Document Control Log

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Change Description | Updated by | Date |
| 0.1 | First Draft Version | Damien Cantelo | 01/08/2023 |
| 0.2 | Draft Revision | Damien Cantelo | 09/08/2023 |
| 0.3 | Draft Revision | Matthew Ingersole | 15/08/2023 |
| 0.4 | Draft Revision | Damien Cantelo | 25/08/2023 |
| 0.5 | Draft Revision | Damien Cantelo | 28/08/2023 |
| 0.6 | Draft Revision | Matthew Ingersole | 29/08/2023 |
| 1.0 | First Published Version | Damien Cantelo | 30/08/2023 |
|  |  |  |  |
|  |  |  |  |