



Data Handling Policy

Cronulla Surf Life Saving Club

September 2026

Contents

Page

1	Purpose	1
2	Scope	1
3	Data Handling	1
4	Data Classification	1
4.1	Restricted Data	1
4.2	Confidential Data	1
4.3	Public Data	2
5	Data Retention & Disposal	2
6	Asset Retention & Disposal	2
7	Media Retention & Disposal	2
8	Cryptography	3
9	Policy Statement	3
9.1	Key Generation	3
9.2	Key Update	4
9.3	Key Storage	4
10	Enforcement	4
11	Revisions	4
12	Document History	5
13	Document Control Log	5

1 Purpose

The purpose of this Policy is to identify what is required to ensure that an appropriate level of assurance and integrity is in place for the handling of data and media as well as the management of cryptographic keys and data encryption. It is used to ensure the proper handling, storage and use of data and cryptographic keys.

2 Scope

This policy applies to all data, media and encryption that are used by Cronulla Surf Life Saving Club (CSLSC). This policy document defines encryption and key management (Certificates) statements that must be used on all applicable mechanisms and systems for CSLSC, whether managed by employees or by third parties. This document forms part of the CSLSC Information Security Policy, and any terms or definitions from that document apply here.

3 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 Confidential and Restricted data is properly managed according to this policy to ensure it doesn't leave the organisation without the necessary authorisation.

4 Data Classification

Data is classified into one of the following three categories:

4.1 Restricted Data

Restricted Data is the most sensitive data classification for CSLSC's data and covers Personally Identifiable Information (PII) which includes a member/employee/contractor's name along with any of the following:

- Government-issued identification numbers (such as {elif country == "Australia" %}Tax File Numbers{% else % Passport Numbers, Driver's License Numbers)
- Credit card numbers
- Financial account data
- Passwords, PINs and other login credentials
- Compensation data (such as salary, bonus, pension)
- Medical data or health status including data about treatment, medical condition or payment for health care
- Insurance or disability data
- Member/employee/contractor location data
- Biometric data such as fingerprints and genetic data
- Data from background checks, including criminal history
- Data related to sexual orientation or behaviour, racial or ethnic background, trade union membership, political opinions or religious beliefs

4.2 Confidential Data

Confidential Data includes Personal Information or Data which is not classified as Restricted Data (as listed above). This would include:

- Member/employee/contractor names
- Member/employee/contractor email addresses
- Member/employee/contractor phone Numbers
- CSLSC pricelists
- CSLSC product specifications
- Unpublished CSLSC materials and content

However, if any of the above data such data is regulated, then it would be reclassified as Restricted Data.

4.3 Public Data

Public Data includes:

- Published marketing materials
- Published content
- Published Annual reports
- Published Press statements
- Public-facing Website data

NOTE: Public Data can sometimes be combined with either Restricted or Confidential Data and should therefore be treated as such to safeguard all data.

5 Data Retention & Disposal

The lifecycle of data handled by the organisation must be managed properly to ensure any Confidential or Restricted data doesn't leave the organisation.

- All member/employee/contractor data must be securely stored for the duration of the service or contract with that member/employee/contractor and must be readily available to ensure the prompt delivery of services to that member/employee/contractor.
- Upon termination of a member/employee/contractor contract, all member/employee/contractor data relating to that member/employee/contractor must be permanently deleted from CSLSC's systems within 3 months of termination.

6 Asset Retention & Disposal

Data may be stored on CSLSC assets such as laptops and computers. The lifecycle of digital assets used by CSLSC must be managed properly to ensure any Confidential or Restricted data doesn't leave the organisation.

- All digital assets must be managed appropriately to avoid data loss, including a thorough data wipe once the asset is no longer in use.

7 Media Retention & Disposal

Data may be stored on storage media from time to time for activities such as data backups, data migration or disaster recovery purposes. The lifecycle of storage media used by CSLSC must be managed properly to ensure any Confidential or Restricted data doesn't leave the organisation.

- All storage media must be used appropriately to securely store data for the period it is required to perform its purpose.
- As soon as the storage media is no longer required, the data must be permanently deleted from the storage media.

Removable media such as USB drives should not be used to store Confidential or Restricted Data.

8 Cryptography

Cryptography is used to encrypt or decrypt data or messages to ensure the confidentiality, data integrity and authenticity in transmission or storage. Cryptography generally uses codes or keys to lock or unlock data using a program or protocol, these can be applied at each end of a transmission or processed against a piece of stored data.

Weak encryption poses a risk of inappropriate access to CSLSC resources. Increases in computing power has enabled people to break weak encryption with commonly and freely available tools and processes. Poor key/certificate management will have a significant impact on availability of systems or service restoration in the event of an incident.

9 Policy Statement

9.1 Key Generation

The following guidelines need to be followed by the MSP during the key generation process.

- Ensure that there is a framework that prevents access or disclosure of cryptographic keys.
- Generate, access, distribute and store data-encrypting keys and key-encrypting keys (a key that is used to encrypt a data-encrypting key) in a controlled and secured manner.
- Consider the impact of using encrypted information on tools which rely upon content inspection such as virus detection tools.
- Ensure encryption standards for external communications are in line with CSLSC encryption standards.
- Ensure that mobile client (application or browser) is encrypting the communication channel while transferring non-public Information or credentials in-line with this policy.
- All Restricted and Confidential Data must be encrypted at rest.
- Must only use AES 256 and higher encryption. Follow FIPS/NIST standards guidelines for encryption technologies.
- Must have encryption and security protocols for the following:
 - a) Sensitive information, including electronic commerce information, transferred over open public networks.
 - b) Sensitive information transported by Mobile or removable media/devices.
 - c) Sensitive information and software exchanged between CSLSC and vendors.
 - d) All non-console system administration access.
 - e) Using 3rd party cloud hosting providers while dealing with Confidential and Restricted Data.
 - f) All remote access connections connecting via the gateway.
- Must require all key custodians to sign a form stating that they understand and accept their key-custodian responsibilities

9.2 Key Update

The following guidelines need to be followed by MSP during the key generation process.

- Must regularly or when circumstances dictate, change all data-encrypting keys and corresponding key-encrypting keys to maintain encryption or key integrity. The following dictates when a key change is required:
 - a) Regular Key Rotation: Keys must be changed at least every year.
 - b) Suspicious Activity: Keys must be changed if they are known to be, or suspected of being compromised.
 - c) Resource Change: Keys must be changed if a resource with knowledge of a clear-text key terminates employment or assumes a new job role that no longer requires access to an encryption process.
 - d) Technical Requirement: Keys must be changed if the key in place has become questionable due to a technical issue such as corruption or instability.
- Must have a process to recover encrypted information in the case of lost, compromised or damaged keys.

9.3 Key Storage

The following guidelines need to be followed by MSP during key generation process:

- Must ensure that when manual clear-text cryptographic key management operations are used that they are managed using split knowledge and dual control.
- Must protect encryption keys from general access. Only approved custodians can access the key components.
- Must authorise custodians to retrieve key components from secure storage or to distribute keys.
- Must store all data-encrypting keys in a secure location and in the fewest number of possible locations and forms.
- Must store key-encrypting keys in physically and/or logically separate locations from data-encrypting keys. In other words, even though there may be an application that needs to have access to both keys, there must be sufficient access controls in place such that a human user does not have access to both, the key-encrypting key and the data-encrypting key.
- Encryption Keys must be stored in a location separate from the encrypted data.

10 Enforcement

Each member of staff is expected to fully comply with this policy. If there is any failure to observe the policy, disciplinary measures may be taken. The measures which may be taken will vary according to the breach and the circumstances of the breach. However, the right is reserved to immediately terminate the employment of any staff member who is in serious breach of this policy or terminate the membership or contract of any member of contractor in serious breach of this contract or terminate the membership or contract of any member of contractor in serious breach of this contract..

11 Revisions

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

12 Document History

Authority

Approved by the Board on (date of effect)	21/09/2026
Due for review on	21/09/2027
Responsible Officeholder for policy	Director Administration
Related legislation/SLSA or SLSNSW or CSLSC policy	
Policy Number	
Signed by Acting Director of Administration (on behalf of Board)	 Annette Tasker (Sep 24, 2026 11:37:30 GMT+10)

13 Document Control Log

Version Control

Version	Details	Date
1.0	Initial draft	September 2026
2.0	Review, update terms and definitions specific to CSLSC	15/09/2026

CSLSC Data Handling Policy v2

Final Audit Report

2026-09-24

Created:	2026-09-24
By:	Kim Grunert (kim.grunert@cronullasurfclub.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAGoTzNJL0BN1tHIKBKpljG-EY2s437wwU

"CSLSC Data Handling Policy v2" History

-  Document created by Kim Grunert (kim.grunert@cronullasurfclub.com)
2026-09-24 - 1:31:53 AM GMT
-  Document emailed to annette.tasker@cronullasurfclub.com for signature
2026-09-24 - 1:32:54 AM GMT
-  Email viewed by annette.tasker@cronullasurfclub.com
2026-09-24 - 1:37:04 AM GMT
-  Signer annette.tasker@cronullasurfclub.com entered name at signing as Annette Tasker
2026-09-24 - 1:37:28 AM GMT
-  Document e-signed by Annette Tasker (annette.tasker@cronullasurfclub.com)
Signature Date: 2026-09-24 - 1:37:30 AM GMT - Time Source: server - Signature Appearance Selected: MOBILE_DRAW
-  Agreement completed.
2026-09-24 - 1:37:30 AM GMT