



Acceptable Use Policy

Cronulla Surf Life Saving Club

September 2026

Contents

	Page
1 Purpose	1
2 Scope	1
3 End User Responsibilities	1
4 IT Team responsibilities	2
5 Monitoring activity and inspection	2
6 Policy Statement	3
6.1 On Induction	3
6.2 During Employment, Membership or Contracting	3
6.3 Internet Usage	3
6.4 Email Usage	4
6.5 Virus Protection	4
6.6 Password Security	5
6.7 Physical Security	5
6.8 Network Security	5
6.9 Incident Reporting & Handling	6
6.10 Travelling	6
6.11 Mobile Computing Devices	7
6.12 Hardware & Software Controls	7
6.11 Personal use	7
7 Enforcement	8
8 Revisions	8
9 Document Information	9
10 Document Control Log	9

1 Purpose

The purpose of this policy is to define acceptable usage for Cronulla Surf Life Saving Club's (CSLSC) information technology (IT) resources and to provide guidance to members, employees and contractors on the proper use of these resources, including use of computer equipment and access to the Internet.

2 Scope

This policy applies to information assets owned or leased by CSLSC and used by members, the Board, officeholders, employees and contractors. To the extent possible, this policy will also apply to devices that connect to CSLSC's network and devices used by visitors at a CSLSC office.

3 End User Responsibilities

- Users are responsible for understanding and following the Information Security policies of CSLSC. Therefore, CSLSC will hold them accountable for their actions.
- Users must not make any unauthorised changes to security settings of the devices under their control.
- Users must not use any of CSLSC's resources to create, send, download or publish material that may be reasonably considered to be illegal, offensive, sexually explicit, discriminatory, defamatory or which incites or promotes violence, contempt or hatred of any group or individual, or which infringes intellectual property (including copyright).
- Users must not transmit any material to any place if that transmission is illegal under the laws of the jurisdiction to which you transmit it.
- Users must not use the CSLSC's resources to harass, bully or discriminate another person. You may be held personally liable for doing so. If you believe you have been harassed, bullied or discriminated against, please contact the Member Protection Information Officer (MPIO).
- Users may only download and install software that have been appropriately licensed for use by CSLSC.
- Users must secure devices via screen lock or logout prior to leaving the area to prevent unauthorised access.
- Users must never store any confidential, sensitive or PII information on local external drives; Such information must be stored in CSLSC's approved Microsoft 365 platforms, including SharePoint and OneDrive, with appropriate security controls and access protections applied. Upon termination of employment, users must return all assigned computing devices and all other computing assets by the end of their last working day.
- Users should respect the computing needs of others by not deliberately performing acts that are wasteful of computing resources or those that unfairly monopolise resources by excluding other users.
- Users are not permitted to use the name of CSLSC's clients in their general communication (email, written or verbal) unless required for the business function.
- Users need to exercise due precautions to ensure that member details or sensitive business information are not discussed in a public place or in any other location where external people might have access to.
- Data stored on local hard drives is susceptible to loss, so users should save their work-related data on CSLSC's Microsoft 365 cloud storage services, including SharePoint and OneDrive, to ensure secure storage, backup, and accessibility.
- Personal software and software downloaded from the Internet should not be installed on CSLSC's computers, unless there is an approved business reason to do so.
- Users shall not use CSLSC's resources (including scanners, printers) for personal use if it will negatively impact business activities or incur more than any nominal cost.
- Users must remove all information from removable media before disposal.

- Users shall not damage, alter or disrupt computer systems.
- All the users should report any observed (or suspected) security weaknesses / incidents to the Managed Service Provider (MSP). Such activities include, but are not limited to, the following:
 - a) Violation of Information Security Policies;
 - b) Breach of confidentiality/ access control;
 - c) Software malfunction;
 - d) Virus activity;
 - e) System failure; and
 - f) Degradation of information processing services.
- All the users must be uniquely identified and authenticated before being allowed to access the Internet. All activities performed under a user's identity will be identifiable and users will be accountable for any activities performed using their identity.
- The use of removable media is on an as-needed basis, including the ability to write to USB drives. If you need to use a USB drive to store any confidential, sensitive or PII information, it must be encrypted. Please contact the Managed Service Provider for assistance.
- The ICT Officer or Managed Service Provider may audit, monitor and log activities, with or without notice, if a situation warrants immediate or further investigation.

4 CSLSC responsibilities

The IT Team must:

- Ensure all equipment has a standard unique identification (other than IP address).
- Maintain a register of all equipment issued to employees, members and contractors and keep the register up to date.
- Setup all devices to comply with all applicable password policies and procedures.
- Remove default passwords for operating systems or applications on all end user computing equipment.
- Synchronise all end user computing device clocks with CSLSC time servers.
- Disable all unrequired services and applications.
- Install and run a personal firewall on all devices.
- Deploy and run anti-malware (virus) software on all devices.
- Ensure all anti-virus/malware tools are current (including definitions) and generate audit logs to a central logging server.
- Patch all devices and ensure devices are completely up to date as per the patch management policy.
- Approve and deploy all software via a service request.
- Place on devices an active password protected screensaver set to activate after a set period of inactivity.
- Only allow trained employees to perform software installation and deployment.
- Maintain end user computing equipment in accordance with the supplier's recommended service intervals and specifications.
- Ensure all information and licensed software is removed or securely overwritten from storage media in all equipment before disposal.

5 Monitoring activity and inspection

By using CSLSC's resources, you consent to CSLSC accessing and monitoring the usage at any time.

- It is a standard function of CSLSC's resources to continuously monitor the activities using to CSLSC's devices. This includes (but is not limited to):
 - a) Phone calls - number dialled, calling number, duration;
 - b) CSLSC emails - sent or received;
 - c) Internet sites – visited, pages accessed, duration, content downloaded;

- d) Documents - accessed, edited, copied, printed;
 - e) Remote access – time of connection, applications accessed, information transferred
 - The activities are backed up as part of CSLSC's standard backup procedures. These backups may be recalled to investigate known or perceived breaches or utilised in legal proceedings or for employees, members or contractors disciplinary purposes.
 - CSLSC may, at any time, use anti-virus and anti-spam software or similar to block, or attempt to block, viruses, spam, malware or any other software which may be considered dangerous to CSLSC's resources.
 - CSLSC may, at any time, block access to certain internet sites or services (e.g. streaming media or instant messaging) which may have an adverse effect on the CSLSC's network performance, bandwidth usage or network security, or which are considered otherwise inappropriate. If you need access to any of these prohibited sites for genuine business reasons you should contact MSP who will arrange access after seeking confirmation of the intended business use from the relevant partner.
 - Unauthorised access to all internal systems is logged and can be tracked.
 - Deleted emails can be accessed for review as may be required by the Legal team.
 - Emails may be subject to discovery and used in legal proceedings.
-

6 Policy Statement

6.1 On Induction

- The employee, member or contractor shall ensure that he/she attends the Information Security training given to the employees on induction.
- The employee, member or contractor shall understand the Information Security Management System of CSLSC
- The employee, member of contractor shall familiarise him/herself with the ways and means to access the information security policies and procedures.
- The employee, member or contractor shall undertake to abide by all the Information security policies and procedures of CSLSC.

6.2 During Employment, Membership or Contracting

- Desktop and laptop computers are for official purpose and shall be used for business purposes only, with the exception of reasonable personal use which doesn't negatively impact business activities or incur more than any nominal cost.
- Users shall use only a reasonable amount of storage on their desktop computers or laptops to store their personal files/data.
- Users shall not use any CSLSC's SharePoint sites, OneDrive accounts, or other Microsoft 365 storage locations to store personal files or personal data.
- Users shall install only approved software on their computer systems.
- The employee, member or contractor shall not use CSLSC facilities for profit making or commercial activity.

6.3 Internet Usage

- Internet connectivity shall be used for official purpose only and shall be driven by the business need, except for occasional personal use out of business hours or during lunchtime.
- While posting any comment on Forums, social media and Internet newsgroups, employees, members and contractors must follow the CSLSC guidelines and direction by the CSLSC Board provided from time to time.
- Users are restricted from accessing hacking, proxy avoidance, peer-to-peer file sharing and pornographic sites, use of instant messengers, downloading of wall papers, screensavers, software applications and other websites that are not required for business purposes, unless expressly permitted by CSLSC.

- Users must not use Internet resources for soliciting business, selling personal products or otherwise engaging in commercial activities other than those expressly permitted which might cause adverse publicity of CSLSC.
- Users must be aware that access to the Internet will be logged and monitored as mentioned in section 5.
- Downloading excessive amounts of data (> 1 GB) has the potential to compromise or disrupt CSLSC's resources. If for business purposes you need to download large amounts of data, please contact the MSP.

6.4 Email Usage

- All Electronic Communications must be professional in nature.
- You must not engage in originating or distributing chain letters by email.
- Email shall not be used for the creation or sending of:
 - Any offensive, illegal, obscene or indecent images or data;
 - Defamatory or which incites or promotes violence, abusive or threatening material;
 - Material that includes false claims of a deceptive nature.
 - Contempt or hatred of any group or individual;
 - Content which infringes intellectual property (including copyright);
 - Junk or unsolicited email received from any other users or external networks.
- Don't open email file attachments received from unsolicited or unreliable sources. Such attachments might contain a virus or a worm.
- Avoid subscription to high volume mailing lists especially if it's not work related.
- You must not transmit any material to any place if that transmission is illegal under the laws of the jurisdiction to which you transmit it.
- Don't use your personal email accounts for CSLSC business communications. Always use your CSLSC corporate email account for this.
- Don't use email casually when dealing with clients and customers. Be aware that email could be used as evidence for legal action.
- You are not permitted to send, on behalf of CSLSC any unauthorised email, attachment or posting to a bulletin board which:
 - Contains information that may have legal implications for CSLSC;
 - Contains commercially sensitive information where users do not have written approval from the CSLSC Board to send such information via email;
 - May damage CSLSC's reputation or its relationships with its clients, or may embarrass its clients;
 - May infringe copyright;
 - May introduce a virus to any of CSLSC's or other networks;
 - Constitutes 'junk' email or is posted to multiple news groups; and
 - Is for private commercial purposes unrelated to CSLSC.
- You are required to undersign emails using your name, job, title and CSLSC name and logo. You should not send any email communication 'for and on behalf of' the CSLSC unless specifically approved to do so.
- Do not send copies of documents /software in violation of copyright laws.
- Do not use email systems for any purpose restricted or prohibited by law or regulations.
- Do not indulge in "spoofing". i.e., constructing an email communication such that it appears to be from someone else.
- Do not indulge in "snooping", i.e., obtaining access to the files or email of others.
- Do not attempt unauthorised access to email or breaching the security measures on any email system.
- Do not send mail addressed to all employees, members or contractors without consulting the CSLSC Board.

6.5 Virus Protection

- Always run the CSLSC's standard anti-virus software.

- Never open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
- Never open any files or macros attached to an e-mail from a known source (even a co-worker) if you were not expecting a specific attachment from that source.
- Be suspicious of email messages containing links to unknown websites. It is possible that the link is a malicious executable (.exe) file disguised as a link. Do not click on a link sent to you if you were not expecting a specific link.
- Never download files from unknown or suspicious sources.
- Do not install freeware /shareware/non-standard software or unlicensed programs onto your systems.
- Avoid direct disk sharing with read/write access unless there is a business requirement to do so.
- Inform MSP for any unusual activities on your systems.
- Do not uninstall the Antivirus software.
- USB drives and other removable storage media shall be scanned for viruses before use.
- All users should minimise the usage of removable media from external sources.
- Any personally-owned devices used on the network must implement virus protection processes and procedures that are in keeping with the standards set out in this policy.
- Regularly update virus protection on personally-owned home computers that are used for business purposes. This includes installing recommended security patches for the operating system and other applications that are in use.

6.6 Password Security

- Never write passwords down.
- Never send a password via email.
- Never tell anyone your password.
- Never reveal your password over the telephone.
- Don't talk about a password in front of others.
- Don't hint at the format of a password (e.g. "my family name").
- Don't reveal a password on questionnaires or security forms.
- Don't share a password with family members.
- Don't reveal a password to co-workers while on leave.
- Never reveal or hint at your password on a form on the internet.
- Report any suspicion of your password being cracked to your MSP.
- If anyone asks for your password, refer them to your MSP.
- Don't use common acronyms as part of your password.
- Don't use common words in part of your password.
- Don't use names of people or places as part of your password.
- Don't use part of your login name in your password.
- Don't use parts of numbers easily remembered such as phone numbers, social security numbers, or street addresses.
- Be careful about letting someone see you type your password

6.7 Physical Security

- Employees must ensure that no unauthorised person enters a working area behind him/her (tailgating).
- Employees shall escort their visitors from and to the reception area.

6.8 Network Security

- Port scanning or security scanning of the CSLSC infrastructure is prohibited, except for the MSP. -

- Executing any form of network monitoring which shall intercept data not intended for the employee's/member's/contractor's host, unless this activity shall be a part of the employee's/member's/contractor's normal job/duty is prohibited.
- Providing information about CSLSC employees, members or contractors to parties outside of the CSLSC without approval is prohibited.
- Don't engage in security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data to which the employee/member/contractor is not an intended recipient or logging into a server or account that the employee/member/contractor shall not be expressly approved to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but shall not be limited to, network sniffing, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

User should not:

- Allow another person to obtain unauthorised access to an information asset by using his/her right of access.
- Reveal one's account password to others or allowing use of one's account by others. This includes family and other household members when work is being done at home.
- Take any external media devices such as USB, CD/DVDs etc. out of the CSLSC. In case of any critical urgency, the request should be raised with the MSP.
- Make unauthorised copies of the software purchased by CSLSC make unauthorised copies of copyrighted material and the installation of any copyrighted software for which CSLSC or the end user does not have an active license.
- Introduce any malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.).

6.9 Incident Reporting & Handling

In case end users observe any unfamiliar activity on their workstation, they shall immediately disconnect the system from the network and report the incident to the MSP or their immediate supervisor. The following steps should be taken by employees/members/contractors on encountering an incident:

- Report any unfamiliar activity on servers/desktops/applications by notifying the MSP by email at support@synergyit.com.au, phone call on 1300 796 796 or verbal communication.
- End users shall comply with the directions given by the MSP to facilitate a quick response, repair of the system, restoring the service and analysis of the incident.

Familiarise yourself with the Incident Management Policy.

6.10 Travelling

Using the CSLSC resources or IT devices while travelling, particularly overseas, presents additional risks. Please note the following:

- Overseas data usage can be costly. Please speak with the Office Manager to ensure that CSLSC does not incur excessive costs.
- Store all the confidential, PII and sensitive information securely while travelling.
- Avoid accessing / working on confidential, sensitive and PII information on public WiFi networks while travelling (public places like airports etc).
- Ensure that the documents that you are reading or writing cannot be viewed by anyone else.
- Don't talk about confidential information relating to business with co-passengers.
- Ensure that your phone conversations are not overheard.

- Never share the username and password used for connecting to the office network or any other system with anybody.

6.11 Mobile Computing Devices

Increasingly, mobile devices are used to store confidential business data. If you are using mobile devices to access, store or transmit CSLSC corporate data, some additional security measures apply. These include:

- Mobile devices must have a PIN code, pattern lock or biometric features (where available) applied and enabled at all times;
- CSLSC corporate data must only be accessed, stored and transmitted using CSLSC approved mobility methods or applications;
- CSLSC corporate data must only be stored using the CSLSC provided secure applications;
- If you lose your mobile device, you must inform the MSP immediately.
- Never leave your laptop, Cellular Phones, Digital diaries, USB Drives etc. unattended.
- Use power-on password for your mobile computing devices.

CSLSC may data wipe (remotely or otherwise) all data (including personal data) from CSLSC-owned mobile devices under the following circumstances.

- The device is reported lost or stolen;
- Your employment with CSLSC is terminated;
- The user has reason to believe that CSLSC corporate data has been compromised;
- CSLSC has reason to believe that the device is compromising the CSLSC technical environment or corporate data.

You should note that data wiping may include personal data stored on CSLSC provided secure applications. Data wiping will be performed through the general course of business where the above scenarios are identified and, in extenuating circumstances, as directed by the CSLSC Board. Where appropriate, you will be notified prior to any data wipe being performed.

6.12 Hardware & Software Controls

- **Hardware Equipment:** Equipment maintained by CSLSC must not be altered or enhanced without the approval of the ICT Officer, whether by users or by approved third-party vendors under a maintenance and/or technical support agreement.
- **Operating Systems Configuration:** Users are not permitted to change operating system configurations, upgrade existing operating systems, apply patches or install new operating systems on CSLSC owned equipment. If such changes are required, they are performed by the MSP only.
- **Application Software:** To request that an application is required for business use (other than standard application of Operating system and MS office); users must submit a request to the MSP. They will perform all installations and upgrades of software. CSLSC reserves the right to perform computer inspections and inventories at any time.

6.13 Personal use

- Subject to compliance with CSLSC's policies, you may use the CSLSC's resources for your own personal purposes out of business hours, provided such use does not have a material adverse impact on the performance of your work or the operation of the CSLSC's resources.
- Please note that CSLSC takes no responsibility for and will not accept liability for use of its resources other than for the purposes of your work at the CSLSC.
- The MSP does not provide support for non-business use of the internet or devices, nor does it provide support for personal mobile devices.

6.14 Artificial Intelligence

Artificial intelligence (AI) tools can assist with club administration and communications, but they also create risk to the confidentiality, accuracy and privacy of CSLSC information. The following requirements apply to any use of AI tools for club business:

- Only AI tools that have been formally approved by the CSLSC Board or the ICT Officer, and that are licensed under a paid CSLSC subscription, may be used for club business. Free, trial, consumer or personally owned AI accounts must not be used for any CSLSC purpose.
- Personally identifiable information (PII) and other confidential or sensitive club information – including member, junior member, employee, health, incident, disciplinary and financial records – must not be entered into, uploaded to, or shared with any AI tool, including approved tools, unless the tool has been specifically approved for that purpose by the CSLSC Board and appropriate data protection and retention controls are in place.
- Where information must be used to complete a task, it is to be de-identified or summarised so that individuals cannot be identified before it is provided to an AI tool.
- Approved AI tools must be accessed using your CSLSC account credentials. Users must not disable, bypass or alter any privacy, data retention or model-training settings configured by the MSP.
- Users remain fully responsible for any output produced with the assistance of an AI tool. All AI-generated content must be reviewed for accuracy, bias, confidentiality and appropriateness before it is used, published, sent externally or relied upon for any decision.
- AI tools must not be used to generate content that would breach any other part of this policy, including material that is offensive, discriminatory, defamatory, misleading, or that infringes intellectual property or copyright.
- AI tools must not be used to make or automate decisions affecting members, employees or contractors without human review and approval through normal club channels.
- Requests to trial or adopt a new AI tool must be submitted to the MSP and approved by the ICT Officer before use.
- Any suspected misuse of an AI tool, or accidental disclosure of CSLSC information to an AI tool, must be reported immediately to the MSP as a security incident in accordance with section 6.9.

7 Enforcement

Each employee, member and contractor 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 employee who is in serious breach of this policy or terminate the membership or contract of any member or contractor in serious breach of this policy.

8 Revisions

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

9 Document Information

Authority

Approved by the CSLSC 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 11:36:31 GMT+10)

10 Document Control Log

Version Control

Version	Details	Date
1.0	Initial draft	September 2026
2.0	Review, update terms and definitions specific to CSLSC	09/092026
3.0	AI usage and controls added to document	12/09/2026

CSLSC Acceptable Use Policy v3

Final Audit Report

2026-09-24

Created:	2026-09-24
By:	Kim Grunert (kim.grunert@cronullasurfclub.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAAbVXi71iHPByWWfKGC8IIRz45ft8oUsH

"CSLSC Acceptable Use Policy v3" History

-  Document created by Kim Grunert (kim.grunert@cronullasurfclub.com)
2026-09-24 - 1:29:41 AM GMT
-  Document emailed to annette.tasker@cronullasurfclub.com for signature
2026-09-24 - 1:31:06 AM GMT
-  Email viewed by annette.tasker@cronullasurfclub.com
2026-09-24 - 1:31:35 AM GMT
-  Signer annette.tasker@cronullasurfclub.com entered name at signing as Annette Tasker
2026-09-24 - 1:36:29 AM GMT
-  Document e-signed by Annette Tasker (annette.tasker@cronullasurfclub.com)
Signature Date: 2026-09-24 - 1:36:31 AM GMT - Time Source: server - Signature Appearance Selected: MOBILE_DRAW
-  Agreement completed.
2026-09-24 - 1:36:31 AM GMT