Information Technology

Acceptable Use Policy

**Umina SLSC**

**September 14, 2023**

Contents Page

[1 Purpose 1](#_Toc142912873)

[2 Scope 1](#_Toc142912874)

[3 End User Responsibilities 1](#_Toc142912875)

[4 IT Team responsibilities 2](#_Toc142912876)

[5 Monitoring activity and inspection 2](#_Toc142912877)

[6 Policy Statement 3](#_Toc142912878)

[6.1 On Induction 3](#_Toc142912879)

[6.2 During Employment 3](#_Toc142912880)

[6.3 Internet Usage 3](#_Toc142912881)

[6.4 Email Usage 4](#_Toc142912882)

[6.5 Virus Protection 4](#_Toc142912883)

[6.6 Password Security 5](#_Toc142912884)

[6.7 Physical Security 5](#_Toc142912885)

[6.8 Network Security 5](#_Toc142912886)

[6.9 Incident Reporting & Handling 6](#_Toc142912887)

[6.10 Travelling 6](#_Toc142912888)

[6.11 Mobile Computing Devices 7](#_Toc142912889)

[6.12 Hardware & Software Controls 7](#_Toc142912890)

[6.11 Personal use 7](#_Toc142912891)

[7 Enforcement 8](#_Toc142912892)

[8 Revisions 8](#_Toc142912893)

[9 Document Information 8](#_Toc142912894)

[10 Document Control Log 8](#_Toc142912895)

# Purpose

This policy aims to define acceptable usage for Umina SLSC’s Information Technology resources and to provide guidance to staff and volunteers on proper use, including the use of computer equipment, access granted to Surf Life Saving systems and access to the Internet.

# Scope

This policy applies to IT assets owned or leased by Umina SLSC and used by Umina SLSC’s staff or volunteers. To the extent possible, this policy will also apply to devices that connect to Umina SLSC’s network and devices used by staff and volunteers at a Umina SLSC office, including bring your own devices (BYOD).

# End User Responsibilities

* Users are responsible for understanding and following the Information Security policies of Umina SLSC
* Users must not make any unauthorised changes to the devices’ security settings under their control
* Users must not use any of Umina SLSC’s IT 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 they share it
* Users must not use the Umina SLSC’s IT resources to harass, bully or discriminate against another person. You may be held personally liable for doing so. If you believe you have been harassed, bullied or discriminated against, please get in touch with the Umina SLSC’s complaints officer
* Users may only download and install software appropriately licensed by Umina SLSC for use on Umina SLSC’s IT resources
* Users must secure devices via screen lock or logout before leaving the area to prevent unauthorised access when unattended
* Users must never store confidential, sensitive or Personally Identifiable Information (PII) on local external drives; instead, they must use a network resource to keep it with the necessary protection
* Upon cessation of a role or membership with a Club or Branch, users must return all assigned computing devices and all other computing assets by the end of their last day in their role
* 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 must exercise due precautions to ensure that members’ details or sensitive Surf Lifesaving information are not discussed in a public place or any other location where external people might have access
* Data stored on local hard drives is susceptible to loss, so users should save their work-related data on Umina SLSC’s network file server or agreed cloud service
* Personal software and software downloaded from the Internet should not be installed on Umina SLSC computers unless there is an approved reason to do so
* Users shall not use Umina SLSC’s resources for personal use if it will negatively impact Surf Lifesaving 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 IT Team. Such activities include, but are not limited to, the following:

1. Violation of Information Security Policies
2. Breach of confidentiality/ access control
3. Software malfunction
4. Virus activity
5. System failure
6. 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 actions performed using their identity
* The use of removable media is on an as-needed basis. It must be encrypted if you need a USB drive to store confidential, sensitive or PII
* The Security Team may audit, monitor, and log activities without notice if a situation warrants immediate or further investigation

# IT Team responsibilities

IT Team must:

* Ensure all equipment has a standard unique identification
* Maintain a register of all equipment issued to staff and keep the record current
* Set up all devices to comply with all applicable password policies and procedures
* Remove default operating system or application passwords on all end-user computing equipment
* Synchronise all end user computing device clocks with Umina SLSC 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 entirely up to date per the patch management policy
* Approve and deploy all software via a service request
* Place an active password-protected screensaver set on devices to activate after a set period of inactivity
* Only allow trained staff to perform software installation and deployment
* Maintain end-user computing equipment by the supplier’s recommended service intervals and specifications
* Ensure all information and licensed software are removed or securely overwritten from storage media in all equipment before disposal

# Monitoring activity and inspection

By using Umina SLSC’s resources, you consent to Umina SLSC accessing and monitoring the usage at any time.

* It is a standard function of Umina SLSC’s resources to continuously monitor the activities using to Umina SLSC’s devices. This includes (but is not limited to):

1. Phone calls - number dialled, calling number, duration
2. Company emails - sent or received
3. Internet sites – visited, pages accessed, duration, content downloaded
4. Documents - accessed, edited, copied, printed
5. Remote access – time of connection, applications accessed, information transferred

* The activities are backed up as part of Umina SLSC’s standard backup procedures. These backups may be recalled to investigate known or perceived breaches or utilised in legal proceedings or for employee disciplinary purposes
* Umina SLSC 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 Umina SLSC’s resources
* Umina SLSC may, at any time, block access to specific internet sites or services (e.g. streaming media or instant messaging) which may hurt the Umina SLSC’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 Surf Lifesaving reasons, you should contact IT, who will arrange access after seeking confirmation of the intended Surf Lifesaving 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

# Policy Statement

## On Induction

* Employees and volunteers must attend the Information Security training during their induction
* Employees and volunteers shall understand the Information Security Management System of Umina SLSC
* Employees and volunteers shall familiarise themself with the ways and means to access the information security policies and procedures
* Employees and volunteers shall abide by all the Information security policies and procedures of Umina SLSC

## During Employment

* Desktop and laptop computers are for official purposes. They shall be used for Surf Lifesaving purposes only, except for reasonable personal use, which doesn’t negatively impact Surf Lifesaving 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 files/data
* Users shall not use any company network location to store their files/data.
* Users shall install only approved software on their computer systems
* Employees and volunteers shall not use Umina SLSC facilities for profit making or commercial activity

## Internet Usage

* Internet connectivity shall be used for official purposes only and driven by the business need, except for occasional personal use outside Surf Lifesaving hours or during lunchtime
* While posting any comment on Forums and social media, employees and volunteers must follow the Umina SLSC guidelines and direction by management provided from time to time
* Users are restricted from accessing hacking, proxy avoidance, peer-to-peer file sharing and pornographic and other websites that are not required for Surf Lifesaving purposes, unless expressly permitted by Umina SLSC
* Users must not use Internet resources for soliciting business, selling personal products or engaging in commercial activities other than those expressly permitted, which might cause adverse publicity of Umina SLSC
* Users must be aware that access to the Internet usage will be logged and monitored, as mentioned in section 5
* Downloading excessive amounts of data has the potential to compromise or disrupt Umina SLSC’s network. If you need to download large amounts of data for Surf Lifesaving purposes, please contact Umina SLSC’s IT Team

## Email Usage

* All Electronic Communications must be professional in nature
* 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 that 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
* 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 share it
* Don’t use your personal email accounts for Umina SLSC Surf Lifesaving business communications. Always use your Umina SLSC corporate email account for this
* Don’t use email casually when dealing with members and volunteers. Be aware that email could be used as evidence for legal actions
* You are not permitted to send, on behalf of Umina SLSC, any unauthorised email, attachment or posting to a bulletin board which:
* Contains information that may have legal implications for Umina SLSC
* Contains commercially sensitive information where users do not have written approval from management to send such information via email
* May damage Umina SLSC’s reputation or its relationships with its clients, or may embarrass its clients
* May infringe copyright
* May introduce a virus to any of Umina SLSC’s or other networks
* Constitutes ‘junk’ email or is posted to multiple newsgroups
* Is for private commercial purposes unrelated to Umina SLSC
* You must undersign emails using your name, job, title, company name and logo. Unless specifically approved, you should not send any email communication ‘for and on behalf of’ the company
* Do not send copies of documents /software violating 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 that appears to be from someone else
* Do not indulge in “snooping”, i.e., obtaining access to the files or emails of others.
* Do not attempt unauthorised email access or breach any email system's security measures
* Do not send mail addressed to all employees and volunteers without consulting the management team

## Virus Protection

* Always run the company’s standard anti-virus software
* Never open any files or documents containing macros attached to an email from an unknown, suspicious, or untrustworthy source. Delete these attachments immediately.
* 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. The link may be 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
* Inform the IT team 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 used for Surf Lifesaving purposes. This includes installing recommended security patches for the operating system and other applications that are in use

## 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 mention the password format (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 online
* Report any suspicion of your password being cracked to your IT team
* If anyone asks for your password, refer them to your IT team
* 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

## Physical Security

* Employees and volunteers must ensure that no unauthorised person enters a working area behind them (tailgating)
* Employees and volunteers shall escort their visitors from and to the reception area

## Network Security

* Port scanning or security scanning of the Umina SLSC infrastructure is prohibited, except for the IT department, when management approves
* Executing any network monitoring that shall intercept data not intended for the employee's host, unless this activity is a part of the employee's regular job/duty, is prohibited
* Providing information about Umina SLSC employees and volunteers to parties outside the company 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/volunteer is not an intended recipient or logging into a server or account that the employee/volunteer shall not be expressly approved to access unless these duties are within the scope of regular duties. For 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 their right of access
* Reveal one’s account password to others or allow use of one’s account by others. This includes family and other household members when work is done at home
* Take any external media devices, such as USBs, CDs/DVDs etc., out of the company. In case of any critical urgency, the request should be raised with the IT Team
* Make unauthorised copies of the software purchased by Umina SLSC, make unauthorised copies of copyrighted material and the installation of any copyrighted software for which Umina SLSC 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.)

## Incident Reporting & Handling

If end users observe any unfamiliar activity on their workstation, they shall immediately disconnect the system from the network and report the incident to the IT Team or their immediate supervisor. Employees and volunteers should take the following steps on encountering an incident:

* Report any unfamiliar activity on servers/desktops/applications by notifying the IT Team via email, phone or verbally
* End users shall comply with the directions given by the IT Team to facilitate a quick response, repair of the system, restore the service and analyse the incident

Familiarise yourself with the Incident Management Policy.

## Travelling

Using the Umina SLSC 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 Umina SLSC does not incur excessive costs.
* Store all confidential, PII and sensitive information securely while travelling.
* Avoid accessing/working on confidential, sensitive and PII information on public Wi-Fi networks while travelling (public places, airports etc).
* Ensure that anyone else cannot view the documents you are reading or writing.
* 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.

## Mobile Computing Devices

Increasingly, mobile devices are used to store confidential Surf Lifesaving data. Some additional security measures apply if you use mobile devices to access, store, or transmit Umina SLSC corporate data. These include:

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

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

* The device is reported lost or stolen
* Your employment with Umina SLSC is terminated
* The user has reason to believe that Umina SLSC corporate data has been compromised
* Umina SLSC has reason to believe that the device is compromising the Umina SLSC technical environment or corporate data

You should note that data wiping may include personal data stored on Umina SLSC 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 senior management. Where appropriate, you will be notified before any data wipe is performed.

## Hardware & Software Controls

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

## Personal use

* Subject to compliance with Umina SLSC’s policies, you may use the Umina SLSC’s resources for your purposes out of Surf Lifesaving hours, provided such use does not have a material adverse impact on the performance of your work or the operation of the Umina SLSC’s resources
* Please note that Umina SLSC takes no responsibility for and will not accept liability for the use of its resources other than for your work at Umina SLSC
* The IT Department does not support non-Surf Lifesaving use of the internet or devices, nor does it support personal mobile devices

# 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 reviewed, tested, and periodically revised as risks, systems, and business practices change.

# Document Information

|  |  |
| --- | --- |
| Title | Acceptable Use Policy |
| Classification | Internal |
| Creation Date | September 14, 2023 |
| Last Review Date | September 14, 2023 |
| Author | Matthew Ingersole |
| Owner | Chief Information Officer |
| Document Number | P-02 |

# 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 | 28/08/2023 |
| 1.0 | First Published Version | Damien Cantelo | 30/08/2023 |
|  |  |  |  |