TITLE: Mobile Device Policy

Purpose

To provide Anglesea Surf Life Saving Club (ASLSC) framework for the effective and efficient use of mobile devices such as tablets, iPhones and iPads to assist with effective communication, provide appropriate security, increase operational efficiency and enhance ASLSC responsiveness and delivery of services to its members and stakeholders.

This includes dealing with ASLSC property, and in particular, in relation to device management, security and privacy.

To provide clear guidelines on what activities are permitted and what activities are restricted thereby ensuring that processes regarding mobile devices assist communication related to ASLSC's business in a flexible and cost-effective manner.

Scope

This policy applies to all ASLSC employees and volunteers regardless of status or position, and any other parties who are issued with an ASLSC owned mobile device and/or tablet device, and/or tablets owned by Life Saving Victoria (LSV) where ASLSC has responsibility for the device.

Hereafter all person covered by this policy are referred to as 'users'.

This policy applies to all ASLSC owned mobile devices that have access to the internet, ASLSC networks, data and information systems and tablets owned by LSV where ASLSC has responsibility for the device. This policy excludes laptops, which are dealt with under the Information Security Policy.

Definitions

Mobile Device - Mobile device is a generic term used to refer to a variety of devices that allow people to communicate and access data and information when mobile. Usually light weight, typically with a touch style screen, this includes mobile phones and tablet style devices.

Jail-broken - to jail-break a mobile device is to remove the limitations imposed by the manufacturer. This gives access to the operating system, thereby unlocking all features and enabling the installation of unauthorised software.

Malware - Malware is any software used to disrupt computer operations, gather sensitive information, gain access to private computer systems or display unwanted advertising.

<u>Internet Service Provider (ISP)</u> - an organisation that provides services for accessing the Internet.

Policy

ASLSC is committed to high standards of data integrity, security and information privacy. This policy reflects that commitment. Mobile devices are essential tools for the day to day business activities of the ASLSC however they can represent a significant risk to the Club if not managed appropriately.

All users issued with a ASLSC owned mobile device are required to adhere to the conditions of this policy for mobile device use, uses should contact the Director of Administration as soon as potential breaches are identified.

Mobile devices and associated services must also be used within the limits of all other ASLSC policies and codes of conduct at all times. Breaching this policy may result in disciplinary action in accordance with ASLSC policies.

Appropriate Use

<u>Connection / Restricted Phone Numbers</u>

ASLSC issued mobile devices must only be connected to ASLSC preferred service providers, on an approved corporate voice call/data plan. Users should not to access 'pay-for-time' telephone numbers unless these are directly related to their work.

<u>Global Roaming</u>

Mobile devices do not have Global Roaming enabled by default. Users issued with ASLSC mobile devices will be liable for any costs associated with Global Roaming unless the use of the device was for ASLSC purposes and approved by the relevant club Director.

<u>Personal Use</u>

Mobile devices have been issued for ASLSC purposes; therefore private usage should be limited. Reasonable personal use of ASLSC provided mobile devices is permitted in recognition of the fact that users may at times need to make personal calls as a result of ASLSC related work or incidental matters.

The authorisation of limited personal use of calls and data of the ASLSC owned device should be discussed and agreed with the relevant Director at the time when the mobile device is issued.

If it is found that a user is operating the device outside agreed reasonable limits for personal use and/or global roaming. ASLSC reserves the right to recover excess personal call and data usage costs from them and/or ask them to return the device.

Security

Mobile devices must not be shared as they store ASLSC information, e.g. emails, calendar, contact information and other information that is confidential. Users are responsible for managing ASLSC data stored on the device and should use reasonable precautions to protect the privacy and confidentiality of ASLSC information stored on the device at all times. This includes preventing others from accessing or using the device in a manner that enables them to obtain ASLSC information to which they would not normally have access. Users must take reasonable care to ensure mobile devices are safely secured at all times to prevent damage, loss, theft or access by unauthorised persons.

Personal Emails

If users wish to use the ASLSC owned device for personal emails they must use a separate ISP and must not merge personal and ASLSC email accounts on these devices. Users must also take particular care to ensure that ASLSC data is only sent through the ASLSC email system.

Wi-Fi

Mobile devices are equipped with Wi-Fi connectivity which by default will be turned on. When the device is in range of ASLSC's Wi-Fi infrastructure, the device will automatically search and connect to the preconfigured Wi-Fi option. When mobile devices come within range of ASLSC's Wi-Fi infrastructure they must be allowed to connect to these systems. Users are required to take care if they use non ASLSC Wi-Fi connections at any time as these services are not supported by ASLSC and may be a security risk.

Use of Mobiles Devices in Vehicles

Under Victorian law, the use of mobile devices while driving is prohibited unless an approved hands-free device or integrated vehicle system connection is used. Accordingly, ASLSC issued mobile devices must only be operated in accordance with prevailing laws. Penalties incurred for failing to comply with the law will be the driver's personal responsibility.

Device Management and Security

Device Management

Devices must:

a) not be "jail-broken" or have any software installed which is designed to gain access to functionality not intended to be exposed to the user.

b) be kept up to date with manufacturer or network provided operating software updates; accordingly, users must regularly check for and install updates.

<u>Repairs</u>

If a mobile device requires repair, the user is to alert the Administration Director prior to repairing the device.

<u>Loss / Theft</u>

Upon determination that a mobile device is damaged beyond repair, lost or stolen please alert the Administration Director.

<u>Change of Position at ASLSC or Leaving the Club</u>

The user must immediately advise the Administration Director when a change in their role at ASLSC no longer entitles them to a mobile device or when they are no longer members of the Club. The device is the be immediately returned to the Administration Director.

Acknowledgment Form

This form asks you to acknowledge that you have read, understood and agreed to adhere to the Anglesea Surf Life Saving Clubs' Mobile Device Policy.

I certify that:

I have read, understood and agreed to adhere to the Anglesea Surf Life Saving Clubs' Mobile Device Policy, in conjunction with Staff Codes of Conduct (as applicable).

I understand that I must complete this acknowledgment form prior to accepting a mobile device;

Use the device for job-related purposes (personal use should be limited);

I must notify the Administration Director immediately upon damage or loss of the device, or when leaving the organisation;

I must properly use the device in regards to voice and data communication;

I have read, understand and agree to adhere to the Anglesea Surf Life Saving Clubs' Mobile Device Policy.

Signed: _____Date: _____

Print Name: _____

Please give this completed Acknowledgment Form to the Administration Coordinator when you obtain your mobile device. A copy will be put on your Personnel File.