Coffs Harbour Surf Life Saving Club

Workplace Surveillance Policy

1 Purpose

Technology improvements have made devices which fall within the statutory definition of surveillance devices commonplace. In the course of normal operations, Coffs Harbour SLSC (the Club) uses these devices and the information and data they generate due to the business benefits they provide. These benefits include, but are not limited to:

- Potential to deter vandalism and/or a possible assailants
- Reduce the safety risks associated with workers, customers and others in the workplace
- Using data and information to defend staff against incorrect allegations
- Increasing information available when conducting investigations (e.g. code of conduct and fraud related complaints)

The Workplace Surveillance Act 2005 (NSW) (WS Act) sets out the legal requirements regarding the use of these devices and information generated by them.

The Purpose of this Policy is to:

- detail the Club's commitment to ensuring that it complies with the requirements of this legislation;
- explain to members, employees, leasees and contractors the types of surveillance that may be carried out in the workplace; and
- explain the responsibilities of management in regards to the introduction of workplace surveillance.

Where there is an inconsistency between this Policy and the WS Act, the WS Act prevails.

2 Who this Policy applies to

This Policy applies to all Club members, employees, leasees and contractors.

This Policy does not form part of any employee's contract of employment nor does it form part of any leasee's lease nor any contractor's contract with the Club.

3 Workplace Surveillance

The WS Act requires the Club to provide notification to its members, employees, leasees and contractors regarding workplace surveillance and prescribes how this notification must be conducted. The following sections of this Policy details the Club's notification:

3.1 Notice of surveillance

This Policy is the written notification to the Club's members, employees, leasees and contractors regarding the Club's activities that fall within the statutory definitions of surveillance.

3.2 Kind of surveillance to be carried out by the Club

The types of workplace surveillance that the Club conducts include:

- Closed Circuit TV Camera surveillance (CCTV)
- Computer surveillance
- Call recording

3.2.1 Camera surveillance

The primary purpose of the Club's camera surveillance is for security. Surveillance cameras are mainly at entries, exits, cash handling areas of the Club facilities and buildings, however some do exist within the Club's offices and other spaces. The Club also uses cameras in spaces where there is public and the Club interaction (e.g. the Club meeting rooms, restaurant and bar areas, etc.). As these spaces are also workplaces, the WS Act applies and the Club will:

- ensure that Surveillance cameras (including their casings or other equipment generally indicating the presence of a camera) are clearly visible where surveillance is taking place.
- clearly display visible signs at each workplace entrance notifying people that they may be under surveillance.

Generally, staff will be aware of and/or involved in the installation of these cameras and this Policy is further notification to staff that these cameras are used.

Access to and use of information or data collected under this Policy is to be in accordance with this Policy.

3.2.2 Computer surveillance

Use of the Club's computers and email and internet accounts generate vital information and data which is considered to be the Club's property and is managed accordingly. The Club may from time to time retrieve and review such information and data in accordance with this Policy.

Examples of information and data that may be accessed and reviewed can include, but is not limited to:

- system storage and download volumes
- internet usage and access
- suspected malicious code or viruses
- email usage including content sent and received
- computer hard drives
- mobile telephone/smartphone/mobile device use, access and locational records (e.g. all telephone bills state the general location calls/texts were made from)
- use of WIFI access points
- access and use of the Club Software
- information and Communication Technology logs, backups and archives
- records from MFDs

The Club will not carry out computer surveillance of an employee unless it is carried out in accordance with this Policy.

The Club reserves the right to prevent (or cause to be prevented) the delivery of an email sent to or from staff, or access to an internet website (including a social networking site) by staff, if it contains, refers or links to material which:

- is obscene, offensive or inappropriate material (for example, material of a sexual, indecent or pornographic nature)
- may causes or may cause insult, offence, intimidation or humiliation
- is defamatory
- may incur liability or adversely impacts the Club's image or reputation
- is illegal, unlawful or inappropriate material
- does or potentially affects the performance of, or cause damage to or overload the Club's computer network, or internal or external communications in any way
- gives the impression of, or is representing, giving opinions or making statements on behalf of the Club without proper delegation

Where an email is prevented from being delivered to or from staff, they will receive a notice that informs them that the delivery of the email was prevented. Notice will not be given if:

- the email was considered to be SPAM, or contain potentially malicious software
- the content of the email (or any attachment) would or might have resulted in an unauthorised interference with, damage to or operation of any program run or data stored on any of the Club's equipment
- the email (or any attachment) would be regarded by a reasonable person as being, in all the circumstances, menacing, harassing or offensive
- an email sent by a user if the Club was not aware (and could not reasonably be expected to be aware) of the identity of the user who sent the email or that the email was sent by the user.

3.3 How the surveillance will be carried out

Surveillance will be carried out in accordance with this Policy.

3.4 When will surveillance start

Where surveillance was already in place prior to this version of this Policy, it will continue. Where surveillance is new, implementation will be 14 days after the approval date of the Policy.

3.5 Surveillance will be continuous

All forms of surveillance (Camera and Computer surveillance) will be continuous and the Club will carry out surveillance of any user at such times of the Club's choosing and without further notice to any user in accordance with the WS Act and this Policy.

3.6 Surveillance will be ongoing

Surveillance, as detailed within this Policy, will be ongoing unless specified within an amendment and subsequent approval of this Policy.

3.7 Changes in technology

As technology improves and changes, other devices are likely to become available and will generate surveillance data and information. Where this happens, devices, information and/or data will be managed in accordance with the WS Act and this Policy.

3.8 Prohibited Surveillance

In accordance with the WS Act the Club will not:

- Conduct surveillance of change rooms and bathrooms.
- Use work surveillance devices while members, employees, leasees and contractors are not at work, unless the surveillance is computer surveillance of the use by the employee of equipment or resources provided by or at the expense of the Club.
- Prevent, or cause to be prevented, delivery of an email sent to or by, or access to an Internet website by, an employee of the Club unless:

- it is in accordance with this Policy

- The Club has (as soon as practicable) provided the employee a prevented delivery notice by email or otherwise, unless notice is not required in accordance with s17(2)-(3) of the WS Act

- Prevent delivery of an email or access to a website merely because:

- the email was sent by or on behalf of an industrial organisation of members, employees, leasees and contractors or an officer of such an organisation, or

- the website or email contains information relating to industrial matters (within the meaning of the Industrial Relations Act 1996 (NSW)).

4 Covert Surveillance

The Club will not carry out, or cause to be carried out, covert surveillance unless it is in accordance with the requirements of Part 4 of the WS Act.

5 Surveillance information and data

All Club staff shall at all times be compliant with the Club's Code of Conduct and maintain strict confidentiality of all Club records, information and data. The Club will ensure that surveillance information and records are not used or disclosed unless the use or disclosure is:

- for a legitimate purpose related to the employment of the Club's members, employees, leasees and contractors or the Club's legitimate business activities or functions, or
- to a member or officer of a law enforcement agency for use in connection with the detection, investigation or prosecution of an offence, or
- for a purpose that is directly or indirectly related to the taking of civil or criminal proceedings, or
- reasonably believed to be necessary to avert an imminent threat of serious violence to persons or of substantial damage to property.

For the avoidance of doubt, the Club may use or rely on surveillance records for the purposes of taking disciplinary or other appropriate action against members, employees, leasees and contractors or investigating a reasonable suspicion that an employee has breached their employment obligations.

Access to CCTV Footage and Surveillance Data

The Club President is the sole release authority for surveillance data and information. In the absence of the President the Club's Director Member Services has the delegated authority of the President to act as the release authority. For clarity, no party may access or review CCTV footage or other surveillance data collected by the Club without the express permission of the Club President or, in the President's absence, the Director Member Services.

If an individual believes they are improperly recorded on CCTV footage held by the Club (ie. not in accordance with this Policy) they can exercise their access rights under privacy or freedom of information legislation, by asking to view or have a copy of the footage. They may exercise this right themselves, or through a legal representative.

All requests for access, with the exception of law enforcement agencies, for CCTV footage must be made in writing and clearly outline the reason for access to: The President, Coffs Harbour Surf Life Saving Club or in his absence The Director of Member Services.

6 Installation of Surveillance Devices

Any installations of surveillance devices must be in-accordance with the WS Act, Surveillance Devices Act 2007 (NSW) and this Policy.

7 Policy breach

Any employee or contractor found to be in breach of this Policy will be subject to appropriate disciplinary action, up to and including summary dismissal.

8 Definitions

Surveillance: of an employee means surveillance of an employee by any of the following means (s3 WS Act): (a) camera surveillance, which is surveillance by means of a camera that monitors or records visual images of activities on premises or in any other place, (b) computer surveillance, which is surveillance by means of software or other equipment that monitors or records the information input or output, or other use, of a computer (including, but not limited to, the sending and receipt of emails and the accessing of Internet websites), (c) tracking surveillance, which is surveillance by means of an electronic device the primary purpose of which is to monitor or record geographical location or movement (such as a Global Positioning System tracking device).

Surveillance information: means information obtained, recorded, monitored or observed as a consequence of surveillance of an employee.

Covert surveillance: means surveillance of an employee while at work for an employer carried out or caused to be carried out by the employer and not carried out in compliance with the requirements of Part 2 of the WS Act.

Workplace: means premises, or any other place, where members, employees, leasees and contractors work, or any part of such premises or place.

9 Key Responsibilities
Overall responsibility of this Policy is with the President.

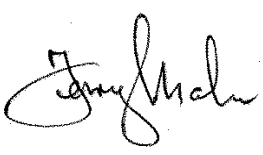
10 References

- Industrial Relations Act 1996 (NSW)
- Local Government Act 1993 (NSW)
- Privacy and Personal Information Protection Act 1998 (NSW) and associated Regulations
- State Records Act 1998 (NSW)
- Surveillance Devices Act 2007 (NSW)
- Workplace Surveillance Act 2005 (NSW) and associated Regulations

11 Details of Approval and revision

- Original Approval Date: 17/01/2019
- Most Recent Review Date: 26/03/19
- Responsible Officer: Club President
- Superseded policies/procedures: NIL
- Next review date: 17/01/2022

Signed by Authoriser:



Terry Maher, Club President **Date: 26/03/2019**