SURF LIFE SAVING
NEW SOUTH WALES

Memorandum

To: Branch President, Directors of Administration & CEO's. Club Presidents & Executive
From: Phil Ayres – Chief Operating Officer
Date: 1 June 2020
Pages: 4
Subject: Surveillance Footage and CCTV's

SLSNSW is aware that many Clubs have CCTV or surveillance cameras in place in and around their Club houses as a means of seeking to ensure greater levels of security. A number of other Clubs are also considering their installation. Finally, SLSNSW has also been asked to provide advice on several grievance matters where the use of CCTV footage was questioned.

The following information is provided to assist Clubs understand their obligations under State legislation with respect to the use of CCTV or surveillance at Club premises. Club Committees and individuals with responsibility for managing the club's CCTV's should be mindful of their personal responsibility in this area.

Please feel free to contact Phil Ayres Chief Operating Officer SLSNSW should you have any questions or require clarification on any of the legislative requirements noted below.

The *Workplace Surveillance Act 2005 (NSW)* (**Act**) was passed in June 2005 and officially came into effect on 7 October 2005. Its purpose is to regulate and outline the legal use of camera, audio, computer surveillance and geographical tracking. Importantly, the Act restricts the use of both overt and covert forms of surveillance.

Under the Act employee has the same meaning as in the *Industrial Relations Act 1996* and includes a person performing voluntary work (that is, a person performing work without remuneration, reward or obligation). Similarly, employer has the same meaning as in the *Industrial Relations Act 1996* and includes a person for whom an employee performs voluntary work.

An employee is at work when the employee is:

(a) at a workplace of the employer (or a related corporation of the employer) whether or not the employee is actually performing work at the time, or
(b) at any other place while performing work for the employer (or a related corporation of the employer).

Volunteers at surf lifesaving Clubs would generally be considered employees. This extends to any time they are at the Club either rostered on for patrol, directing training (eg bronze medallion courses), attending training (surf sports or lifesaving), coaching surf sports or attending the Club and surrounds casually.

The Act limits the use of surveillance devices in the workplace by prohibiting an employer from carrying out or causing to be carried out any surveillance of an employee in a:

- change room
- toilet facility
- shower or bathing facility.

The Act also requires notice to be given to employees at least 14 days prior to surveillance commencing which includes details of:

- the type of surveillance to be carried out
- how the surveillance will be carried out
- when the surveillance will commence
- whether the surveillance will be continuous or intermittent
- whether the surveillance will be for a specified limited period or ongoing.

The Act also contains specific provisions in relation to the need for notices on vehicles that are the subject of tracking, computer monitoring policies, notices identifying that cameras are operating in the workplace and the visibility of the cameras in the workplace.

Disclosure and use of surveillance records is specifically regulated in NSW. To disclose surveillance records in NSW one of the following conditions must be met:

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

Overt Surveillance

Overt surveillance occurs when employers surveil employees, with the employees notified of this action. Under the Act, overt surveillance is unlawful unless notice has been given in advance (minimum 14 days before surveillance starts). Additionally, new employees must be notified before they start work. The notice must contain details of:

- What kind of surveillance is going to be used (video, audio, tracking);
- When the surveillance will commence;
- Whether the surveillance will be intermittent or continuous; and
- Whether the surveillance will be for a specific time or ongoing.

Furthermore, all surveillance is required to be placed in clearly visible places with signs indicating surveillance is taking place.

Covert Surveillance

Covert surveillance refers to surveillance that is undertaken without the knowledge of the employee(s). The Act strictly prohibits covert surveillance unless the employer obtains a 'covert surveillance authority' which has been issued by a Magistrate authorising the surveillance to determine whether the employee(s) are involved in unlawful activity at work.

When issuing a covert surveillance authority, the Magistrate will consider the following:

- The seriousness of the unlawful activity;
- Whether it will affect the right to privacy of other employees in the area; and
- Whether reasonable grounds exist to justify the surveillance authority.

Tracking & GPS Surveillance

The Workplace Surveillance Act also regulates all forms of tracking surveillance on employees including electronic devices which monitor an employee's geographical location such as GPS. If an employer intends to track an

employee using a vehicle i.e. GPS tracking of the Club SSV, a clearly visible notice must be displayed on the vehicle to indicate that the vehicle is subject to tracking surveillance.

Computer, Internet and Email Surveillance

The Act restricts computer surveillance by employers including monitoring or recording of information accessed and sent. It also regulates the surveillance of internet access by employees and prohibits the blocking of emails.

Under the Act, surveillance of an employee's computer use can only be carried out where:

- There is an existing policy on computer surveillance in the workplace; and
- Notice has been given to the employee in advance; and
- The employee is aware of and understands the policy.

The Act also prohibits the blocking of emails sent to or by an employee. Emails will be blocked if it is in accordance with the computer policy of the workplace, the content of the email contained a virus, was spam or can be reasonably regarded as being menacing, harassing or offensive.

Prohibited Surveillance Areas

Aside from the above regulations, the Act specifically prohibits surveillance in certain areas. As noted above these include change rooms, toilets, showers or bathing facilities at a workplace.

The Act means employers need to ensure that the surveillance systems they have in place are in accordance with legislation. The Act provides employees protection from surveillance that infringes on their right to privacy and facilitates a safe working environment.

Members who believe they have experienced unlawful surveillance at their SLS Club or would like the existing workplace/SLS Club policies reviewed, have a right to contact and raise these issues with their respective Club. Club Committees are required to be responsive to these requests and where they are uncertain of the correct approach should contact SLSNSW for advice.

Provision of Footage to Members and Other People

The Club policy around whom and when individuals have access to any CCTV footage should be clear. Only designated persons in an official capacity should have access to CCTV footage and stored files/tapes. The number of persons should be limited. These images must not be provided to any third parties or members of the Club unless under a legal order or police request.

For the purpose of identifying individuals (eg the theft of an item picked up by a CCTV camera), designated officials may show third parties and/or Club members the specific footage in question, but are not allowed to provide these individuals direct copies of these images, screen shots, or allow the filming of them off the screen by another camera (eg a phone).

Club Policy

All clubs should have a policy on the use of CCTV's and/or any other surveillance they are undertaking of members. The policy must be available to all member to view. A sample policy is available on the SLSNSW website.

Installation Approval

Clubs should be aware that in most circumstances it will be a requirement of their lease agreement with the building owner (eg Local Council) to seek approval to install and/or use any CCTV/Surveillance cameras prior to installation. Clubs should review their lease agreement and liaise with their building owner.

SURF LIFE SAVING NEW SOUTH WALES

SAMPLE SURF LIFE SAVING CLUB (SLSCs)
CCTV CAMERAS POLICY

POLICY GUIDELINES

To assist in providing a safe physical environment some SLSCs in New South Wales have installed a CCTV surveillance system at their Club premises. The area covered at each Club differs.

This policy has been developed to govern the use of CCTV cameras at SLSCs.

PURPOSE

The purpose of this policy is to govern the use of a CCTV system by XXX SLSC as an incident risk management tool under the requirements of the *Work Health and Safety Act 2011 (NSW)* (**WH&SA**) as well as the *Workplace Surveillance Act 2005 (NSW)* (**WSA**).

SCOPE

These guidelines focus only on the use of CCTV cameras at XXX SLSC which operate in the XX, XX and XX areas of the club house

The operation of CCTV is regulated by sections 11, 14 and 16 of the WSA and the following requirements:

- CCTV cameras will be clearly visible.
- Signs will be at each entrance to notify people that they may be under surveillance.
- SLSCs will not use CCTV to conduct surveillance of employees who are not at work. Employees include volunteers. An employee will be considered to be "at work" when they are at the workplace of the employee or they are anywhere else whilst performing work for the employer.

LEGISLATIVE FRAMEWORK

WSA

The WSA applies to camera surveillance, computer surveillance and tracking surveillance of staff or in XXX SLSCs' case members. The Act regulates the use of both overt and covert surveillance and the use and disclosure of the records obtained from surveillance.

Surveillance Devices Act 2007 When conducting workplace camera surveillance, if the camera is used to record private conversations, the camera surveillance will also be regulated by the Surveillance Devices Act 2007 *(NSW)*.

Privacy legislation

Personal information collected by surveillance will be protected by the *Privacy and Personal Information Protection Act 1998 (NSW)*.

Guidelines

XXX SLSC will operate only overt camera surveillance to observe personal or property security and unlawful activity.

OVERT CAMERA SURVEILLANCE

Employee Notification

Section 10 of the WSA provides clear direction on the requirements for notifying employees where an employer wishes to undertake overt workplace camera surveillance.

The use of cameras to undertake workplace surveillance will be lawful under the WSA only if all of the following conditions are met:

- employees have been notified, in writing, at least 14 days before the cameras are used. New starters (including new members and new paid employees) must be advised prior to commencing work (section 10);
- the cameras are clearly visible to people in the area that is under surveillance (section 11); and
- signs notifying people that they may be under camera surveillance are clearly visible at each entrance to the area under surveillance (section 11).

Notification Exemption Clause

Section 14 of the WSA allows for an exemption from the employee notification requirements where the surveillance is:

- conducted with the agreement of the employee or a body representing a substantial number of employees at the particular workplace e.g. a union or representative body, for a purpose other than surveillance of members and the public near or on the SLSC premises (e.g. security purposes) and
- carried out in accordance with that agreement.

Failure to meet all the requirements for overt surveillance will constitute covert surveillance, which is in breach of the Act in the absence of a covert surveillance authority.

Security related workplace camera surveillance

In a security context, camera surveillance is generally used to:

- deter security incidents e.g. theft, vandalism, violence, etc;
- gather information that may be used in evidence if a crime is committed within view of the camera (assuming the camera is recording);
- allow a security incident to be viewed as it is occurring and an appropriate response to be raised.

MONITORING OF CAMERA SURVEILLANCE

Where continuous monitoring of CCTV at SLSCs is not feasible the following strategies, as a minimum, should be considered:

- the CCTV is continuously recorded with archived images stored for up to 7 days;
- a physical security response is mobilised where an alarm is activated;
- protocols advising XXX SLSC officers if an incident occurs are established;
- regular review of the effectiveness of the above strategies is undertaken to ensure risk and liability are being appropriate managed in a way that maintains the security of the SLSC.

PLACEMENT OF CAMERAS

Where a security risk assessment results in the decision to use overt camera surveillance in a particular location, effective placement of the camera within this location is critical to the success of a surveillance strategy aimed at controlling security risks.

- Lighting levels, including shadowing, minimum lux levels, type and height including varying lighting levels in open areas as opposed to under awnings etc and obstructions to fields of view.
- Pedestrian thoroughfares, including analysis of the amount of pedestrian access throughout each day.
- The recommended height of equipment above ground to deter potential vandalism (while noting that position height of cameras needs to allow adequate identification of persons.
- The view from the recommended camera height, taking into account building structures and awnings.
- Direction of the sun, including sunrise and sunset 'blooming' and the possible effect on the cameras.
- Whether private premises would come within the view of the cameras.
- The accessibility of equipment for maintenance purposes including any safety issues for members or contractors undertaking the maintenance.
- Possibility of accompanying lighting intruding upon the surrounding area. Access to power supply.
- Cabling routes and distances.
- Availability of existing cables and conduits.

RELATED PROCEDURES

XXX SLSC should also consider:

- Ensuring camera surveillance equipment remains appropriately placed, and continues to be pointed in the necessary direction.
- Maintenance and testing of the equipment - a maintenance log is recommended. The CCTV system and any alarms should be regularly tested.

- Undertaking regular risk assessments to ensure that the introduction of camera surveillance has not created new or different security risks e.g. moved potential illegal activity from the area now under surveillance to other surrounding areas, or created expectations in relation to a duress response that may be unrealistic or unable to be met.

USE AND DISCLOSURE OF SURVEILLANCE RECORDS

The WSA requires that any record made as a result of surveillance not be used or disclosed unless the disclosure is:

- For a legitimate purpose related to the legitimate business activities of XX SLSC.
- To a member or officer of a law enforcement agency (eg Police) for use in connection with the detection, investigation or prosecution of an offence.
- For a purpose that is directly or indirectly related to the taking of civil or criminal proceedings.
- Reasonably believed to be necessary to avert an imminent threat of serious violence or of substantial damage to property.

As it is in the public interest to assist law enforcement agencies to pursue their law enforcement and public protection activities, XXX SLSC should assess requests for surveillance records in the absence of a warrant on a case by case basis.

In deciding whether to provide surveillance records XX SLSC should balance this need with its own obligations of confidentiality to its members and the sensitive nature of legal information.

Factors that should be considered prior to disclosing surveillance records without a warrant include:

- The seriousness of the alleged offence.
- The degree of evidence available that suggests the surveillance record contains information that will assist with law enforcement.
- Whether significant personal information relating to third parties will be disclosed.
- How well sign posted the camera surveillance is i.e. will members and visitors to the area have a reasonable expectation that they will be captured in surveillance records.
- Any industrial arrangements as the surveillance records may also include footage of members.