



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.