



---

**NAME OF POLICY:**        **Surveillance Device Policy**

---

**POLICY MANUAL:**        **HR Manual**

---

## **BACKGROUND**

The Council is authorised under the *Surveillance Devices Act 2016 (SA)*, to use *Surveillance Devices* in various circumstances.

*Surveillance Devices* can be divided into four (4) primary categories, as set out below:

- *Listening Devices*: a device capable of being used to listen to or record a private conversation or words spoken to or by any person in private conversation;
- *Optical Surveillance Device*; a device capable of being used to observe or record visually (whether moving picture or not) a person, place or activity;
- *Tracking Device*: a device capable of being used to determine the geographical location of a person, vehicle or thing; and
- *Data Surveillance Device*: a program or device capable of being used to access, track, monitor or record the input of information or the output of information from, a computer.

The objective of this Policy is to set out the circumstances in which the Council will use *Surveillance* and ensure all staff, contractors, Volunteers and members of the community are informed.

## **DISCUSSION**

The Council has determined that in some circumstances, it is appropriate to install, use or maintain *Surveillance Devices*.

## **POLICY**

### **Objectives**

The objectives and use of *Surveillance Devices* by the Council are to:

- obtain accurate records of meetings, conferences and conversations including Council, Committee, staff and other meetings;
- enhance the integrity of records management through the use of *Data Surveillance Devices*;
- ensure the safety of workers and citizens while present in monitored areas and/or while using Council equipment, vehicles, plant and goods;
- protect and ensure the appropriate use of Council equipment, vehicles, plant, goods, computers, programs and workplace areas;
- use data which is obtained from *Surveillance Devices* to support proceedings involving external parties (e.g. enforcement proceedings for alleged offences by members of the public);
- use data which is obtained from *Surveillance Devices* to support internal investigations or proceedings involving internal parties (e.g Behaviour Standards complaints and other workplace investigations or proceedings).

## **Installation of a Surveillance Device**

Installation of any *Surveillance Device* must be approved by the Chief Executive Officer or a staff member who is delegated by the Chief Executive Officer to do so, in consultation with the Manager, Organisational Development. Installation of a *Surveillance Device* must only be for a purpose which is permissible under the *Surveillance Devices Act 2016* and within requirements of this Policy.

The Chief Executive Officer (or delegate) who approves the installation of a *Surveillance Device* will only do so once the conditions which apply to the use and maintenance of the *Surveillance Device* have been determined and documented in writing, at the time of approving the installation of the *Surveillance Device*. These conditions may be revised from time-to-time by either the Chief Executive Officer (or delegate), and any revision of an installation will be documented in writing. This does not compromise those *Surveillance Devices* that have been installed by the Council prior to the *Surveillance Device Act* being enacted.

In the event that a *Surveillance Device* is to be installed for the main purpose of protecting the lawful interest of the Council and therefore may be for the purpose of observing the conduct and action of a specific staff member, the Chief Executive Officer and the Manager, Organisational Development must establish sufficient cause to do so and the installation of the *Surveillance Device* must be approved by the Chief Executive Officer and the Manager, Organisational Development. In the event the *Surveillance Device* is to be installed to protect the lawful interest of the Council and is to be used to observe the conduct and action of the Chief Executive Officer, the Mayor and the Manager, Organisational Development must establish sufficient cause to do so and the installation of the *Surveillance Device* must be approved by the Mayor and the Manager, Organisational Development

Except insofar as it may compromise or adversely affect an effort to protect the lawful interest of the Council or another person, the Chief Executive Officer or Delegate will ensure that the relevant General Manager and Manager are advised of:

- the installation and nature of the *Surveillance Device*; and
- the conditions which apply regarding the use and maintenance of the *Surveillance Device*.

Any unauthorised installation, use, maintenance tampering or removal of a *Surveillance Device*, will be treated as serious misconduct by the Council. Such actions by any member of staff may result in Disciplinary Action, including termination of employment.

## **Use and Storage of Data obtained from a Surveillance Device**

Data obtained from a *Surveillance Device* will be collected and used only:

- for a purpose which is permissible under the *Surveillance Device Act* and within the contemplation of this Policy; and
- in accordance with any privacy obligations which apply from time to time.

Data obtained from a *Surveillance Device* which constitutes an official record will be stored and disposed of in accordance with the *State Records Act 1997 (SA)*.

Data Obtained from a *Surveillance Device* are subject to the operation of the *Freedom of Information Act 1991 (SA)*, including any exemptions which may apply (such as, for example, documents affecting law enforcement and public safety, and documents affecting personal affairs).

Data obtained from a *Surveillance Device* in respect of any staff member, may only be accessed by:

- the Chief Executive Officer;
- the Manager to whom the staff member reports (but only if authorised to do so by the Chief Executive Officer);
- the General Manager to whom the staff member reports (but only if authorised to do so by the Chief Executive Officer);
- the Manager, Organisational Development;
- any person who has been authorised specifically in writing by the Chief Executive Officer to access that data, and only for the purpose and to the extent described in the written authorisation;
- in respect of data obtained from a *Data Surveillance Device* - the Manager, Information Services, provided that the Manager, Information Services notifies and obtains approval from the Chief Executive Officer;
- any contractor engaged to provide services in connection with the installation, use or maintenance of a *Surveillance Device*, in accordance with the applicable terms of engagement; and
- any legal advisor who is appointed by the Council.

Any unauthorised access, misuse, disclosure, tampering, copying or removal in relation to data obtained from a *Surveillance Device* will be treated as serious misconduct by the Council. Such actions by any member of staff may result in Disciplinary Action, including termination of employment.

### **Listening Devices**

Under the *Surveillance Devices Act 2016*, the Council may install, use or cause to be used, or maintain a *Listening Device* to monitor or record any conversation:

- made in circumstances in which all parties to the conversation ought reasonably to expect that the conversation may be heard by a person who is not a party to the conversation; or
- where no party to the conversation could, in the circumstances, reasonably be taken to desire the conversation to be heard only by parties to the conversation.

Additionally, under the *Surveillance Devices Act 2016*, if the installation, use or maintenance of a *Listening Device* on or within a premises or a vehicle is reasonably necessary for the protection of the lawful interests of the Council or the owner, or occupier of the premises or vehicle or some other person, the Council may so install, use or maintain a *Listening Device* on or within:

- premises or a vehicle of which the Council is an owner or occupier;
- other premises or another vehicle, provided an owner or occupier of the premises or vehicle agrees to the installation, use or maintenance of the *Listening Devices*.

Examples of lawful interests which the Council is entitled to protect are set out in this Policy.

### **Optical Surveillance Devices**

Under the *Surveillance Devices Act 2016*, the Council may install, use or maintain an *Optical Surveillance Device* on or in premises, a vehicle or other thing to record visually or observe the carrying on of any activity (involving one or more persons):

- carried on in a public place; or
- carried on in a premises or a vehicle if the activity can be readily observed from a public place; or
- carried on in a circumstance in which at least one party to the activity ought reasonably to expect that the activity may be observed by a person who is not a party to the activity; or
- where no party to the activity could, in the circumstances, reasonably be taken to desire the activity to be observed only by parties to the activity.

Additionally, under the *Surveillance Device Act*, the Council may install, use or maintain an *Optical Surveillance Device* on any Council premises (including building, parks, reserves, roads, vehicles etc), if the use of the device is reasonably necessary for the protection of the lawful interests of the Council.

Examples of lawful interests which the Council is entitled to protect are set out in this Policy.

### **Lawful Interests**

Lawful interests which the Council is entitled to protect through the installation, use or maintenance of *Listening Devices* and *Optical Surveillance Devices* (where it is reasonably necessary to do so) include the following:

- protection of information from misuse, mismanagement, tampering, improper disclosure, or loss;
- protection of resources (including financial resources), goods, equipment, vehicles and plant from misuse, mismanagement, tampering, theft including timesheet fraud, damage and loss;
- prevention, detection or investigation of potential corruption, misconduct or maladministration in public administration; or
- prevention, detection or investigation of other potential offences or misconduct which may arise in connection with, or may impact upon, the affairs or operations of the Council.

### **Placement of Listening Devices and Optical Surveillance Devices**

Without derogating from the above provisions, the Council gives specific notice that *Listening Devices* and *Optical Surveillance Devices* may be installed, used and maintained in the following places:

- Customer Service areas and other workplace areas where members of the public are permitted to access;
- external public areas;
- workplace areas including hallways, office areas, sheds and yards (but, for the avoidance of doubt, *Optical Surveillance Devices* will not be used in any restroom or changing room);
- Council owned telephones may be used to record conversations (but, for the avoidance of doubts a private conversation with a member of the public who is not subject to this policy may only be recorded with the express or implied consent of the member of public).

Specific locations of *Listening Devices* and *Optical Surveillance Devices* will be advised to any staff member, contractor or Volunteer upon request to the relevant Manager or General Manager to whom that staff member, contractor or Volunteer reports, except where disclosure of any specific device and/or location may compromise or adversely affect an effort to protect the lawful interest of the Council or another person.

### **Tracking Devices**

The Council may install, use or maintain a *Tracking Device* to determine the geographical location of any vehicle or thing, (including any movable equipment or plant):

- owned by, or in the lawful possession or lawful control of, the Council; or
- owned by, or in the lawful possession or lawful control of, another person, provided the owner or a person in lawful possession or lawful control of the vehicle or thing provides express or implied consent to the installation, use or maintenance of the *Tracking Devices*.

In exercising this entitlement under the *Surveillance Devices Act 2016* to install, use or maintain a *Tracking Device* to determine the geographical location of a vehicle or thing, the Council may, by inference, determine the location of any driver, operator, passenger or user of the vehicle or thing. By driving, operating, travelling in, or using any vehicle or thing owned by or in the lawful control or possession of the Council (including a rental), a worker acknowledges and consents to the presence and use of a *Tracking Device* in or on that vehicle or thing, which may be used to determine geographical location of the vehicle or thing and, by inference, the staff member.

*Tracking Devices* include:

- Global Positioning Systems (GPS) devices and equipment and similar devices and equipment;
- other telematics/ telemetry (e.g. speed, acceleration, fuel usage, activation of equipment/functions) to the extent that such telematics/telemetry may be used to determine or impute geographical location;
- tablet computers and mobile telephones (including where location data are directly available as a function of the device, and where location data can be inferred from information or other data from a utility or other service provider); and
- security and access technology requiring the scanning of key cards or the entering of codes, credentials or other information.

### **Data Surveillance Devices**

The Council may install, use or maintain *Data Surveillance Devices* to access, track, monitor or record the input of information into, the output of information from or information stored in, a computer:

- owned by, or in the lawful control or management of, the Council; or
- owned by, or in the lawful control or management of another person, provided the owner or person in lawful control or management of the *computer* provides express or implied consent to the installation, use or maintenance of the *Data Surveillance Device*.

The term '*computer*' includes:

- desktop and laptop computers;
- tablet computers and mobile telephones;
- other mobile computers including scanners, expiation and enforcement, computers, and digital cameras;
- payment terminals and other technology associated with receipt, payment or management of money; and
- security and access technology requiring the scanning of key cards or the entering of codes, credentials or other information.

### **Other Authority**

Nothing in this Policy limits the ability of a staff member to use a *Surveillance Device* which is consistent with the authority under other legislation (including the use of microphones and cameras for investigative or enforcement purposes by officers authorised under relevant legislations).

### **Public Surveillance**

Nothing in this Policy limits the ability of the Council to install, use or maintain any *Surveillance Device* in accordance with the *Surveillance Devices Act 2016* for the purpose of monitoring a public area.

## RELATED POLICIES

This Policy should be read in conjunction with the following Policies:

- Behaviour Standards Policy
- Fair Treatment and Equal Opportunity Policy
- Disciplinary & Under-Performance Policy
- Social Media & Electronic Communication Policy
- Electronic Communication Devices Policy

## REVIEW PROCESS

The Council will review this Policy within 36 months of the adoption date of the Policy.

## INFORMATION

The contact officer for further information at the City of Norwood Payneham & St Peters is Council's Manager, Organisational Development, telephone 8366 4564 or email [nnewton@npsp.sa.gov.au](mailto:nnewton@npsp.sa.gov.au).

## ADOPTION OF THE POLICY

This Policy was adopted by the Chief Executive Officer on 5 July 2018.

## TO BE REVIEWED

30 June 2021



---

Mario Barone  
**CHIEF EXECUTIVE OFFICER**

5 July 2018

---

Date