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 City Council (Council) 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
- Optimise efficiency and customer service
- Gather operational data for workforce and fleet management efficiency gains (e.g. work allocation and route improvements)
- Identifying geographical location of a worker in the event of an emergency
- 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, defending Council)
- Assist in scheduling and allocation of tasks to work teams

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

The purpose of this Policy is to:

- detail Council's commitment to ensuring that it complies with the requirements of this legislation;
- explain to employees 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 Council employees and contractors, and at all Council premises.

This Policy does not form part of any employee's contract of employment nor does it form part of any contractor's contract with Council.

3 Workplace Surveillance

The WS Act requires Council to provide notification to its employees regarding workplace surveillance and prescribes how this notification must be conducted. The following sections of this Policy details Council's notification.

3.1 Notice of surveillance

This Policy is the written notification to Council employees regarding Council's activities that fall within the statutory definitions of surveillance.

3.2 Kind of surveillance to be carried out by Council

The types of workplace surveillance that Council conducts include:

- Closed Circuit TV Camera surveillance (CCTV)
- Computer surveillance
- Tracking surveillance

3.2.1 Camera surveillance

The primary purpose of Council's camera surveillance is for security. Surveillance cameras are mainly at entries, exits and around the exteriors of Council facilities and buildings, however some do exist within Council's Offices. Council also uses cameras in spaces where there is public and council interaction (e.g. Council Chambers, customer service areas, library, art gallery etc.). As these spaces are also workplaces, the WS Act applies and Council 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.

Council has in car dash cameras within the Ranger's vehicles which can also record audio within the vehicle. Council will clearly display a notice within each vehicle indicating that it has an in car dash camera which can also record audio.

Council also installs surveillance cameras in and near worksites, plant and fleet to monitor out of hours security when a site is unoccupied (e.g. identify plant, equipment and fuel theft). These cameras are:

- not operated during work times as security risks are lower due to the presence of staff
- unlikely to have signage

Generally, onsite 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 collected using camera surveillance is to be in accordance with the Video Surveillance on Public and Other Lands Policy.

3.2.2 Computer surveillance

Use of Council's computers and email and internet accounts generate vital information and data which is considered to be Council's property and is managed accordingly. Council 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 phone bills state the general location calls/texts were made from)
- use of WIFI access points
- access and use of Council Software
- information and Communiction Technology logs, backups and archives
- records from MFDs

Council Business Systems staff are approved to monitor the above to maintain network stability, continuity of service and compliance.

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

Council 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:

- obscene, offensive or inappropriate material (for example, material of a sexual, indecent or pornographic nature)
- material that causes or may cause insult, offence, intimidation or humiliation
- defamatory or may incur liability or adversely impacts Council's image or reputation
- illegal, unlawful or inappropriate
- anything that does or potentially affects the performance of, or cause damage to or overload Council's computer network, or internal or external communications in any way
- anything that gives the impression of, or is representing, giving opinions or making statements on behalf of Council 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 Council'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 Council 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.

Group Leader Business Systems has responsibility for access and use of data collected via computer surveillance carried out in accordance with this section.

Employee's and contractor's obligations when using Council's computers and other IT resources are set out in Council's Resource Data Management, Monitoring and Use Procedure (Name of document to be confirmed).

3.2.3 Tracking surveillance

Council uses devices and technology that has tracking capability including but not limited to:

- GPS tracking within Council vehicle, truck and plant fleet
- Council supplied radios (including those used for isolated worker management)

- "On person" isolated worker devices
- Council issued mobile phones, smart phones, tablets and computers with GPS/WIFI capability

This data will be used for (but not limited to):

- planning and scheduling works
- monitoring performance data for maintenance and repair requirements
- knowing the location of plant, fleet and staff to reduce response times to customer requests and emergency works
- monitoring travel to identify opportunities to increase tool time
- identify staff, plant and fleet locations and respond to emergencies
- investigations due to complaints, customer requests and incidents
- information availability and access requirements

Where a vehicle, truck, plant or other item has tracking capability, Council will clearly display a notice on the item indicating that it is subject to tracking surveillance.

Both Group Leader Infrastructure Construction and Maintenance and Group Leader Financial Services and Logistics has responsibility for access and use of data collected via tracking surveillance carried out in accordance with this section.

Employee's obligations when using Council's plant and fleet are detailed in Council's Vehicle and Plant Use Procedure. Council's isolated worker Management is detailed in the Isolated Worker Procedure.

3.2.3.1 Infrastructure Construction and Maintenance plant and fleet

In addition to the above, Operational Plant and Fleet tracking data will be displayed on a screen at Council's main depots and monitored in real time by relevant staff for the purposes of scheduling and allocation of work.

Further, maintenance scheduling and workshop staff will have access to Plant and Fleet performance and usage data, collected via tracking surveillance, in order assist in priorisiting and scheduling maintenance and repair to improve efficiency and maintenance management.

3.2.3.2 Isolated Workers

Council' "On person" isolated worker devices (i.e. man down) are used to identify the location of an isolated/remote site worker in an emergency. Staff required to use these will be informed that they are required to carry the device whilst working alone at work.

Council' "On person" isolated worker device data and information will be accessible, retrieved and used without further authorisation in the following circumstances:

- A worker fails to return to base at the expected time
- A worker does not respond to repeated attempts to contact them.
- A pendant alarm is activated.
- A tilt switch alarm is activated.
- A portable radio panic button is activated.
- An emergency situation requires the ability to locate council vehicles.

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, Computer and Tracking surveillance) will be continuous and Council will carry out surveillance of any user at such times of Council'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

Council will not, in accordance with the WS Act:

- Conduct surveillance of change rooms and bathrooms
- Use work surveillance devices while employees 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 Council.
- Prevent, or cause to be prevented, delivery of an email sent to or by, or access to an Internet website by, an employee of Council unless:
  - it is in accordance with this Policy
  - Council 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 employees 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

Council 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 Council staff shall at all times be compliant with Council's code of Conduct and maintain strict confidentiality of all Council records, information and data. Council 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 Council employees or Council'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 Council may use or rely on surveillance records for the purposes of taking disciplinary or other appropriate action against employees or investigating a reasonable suspicion that an employee has breached their employment obligations.

Access requests outside of this Policy are to be made in accordance with the relevant Surveillance data access procedure(s).

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 employees work, or any part of such premises or place.

9 Key Responsibilities

Overall responsibility of this Policy is with the General Manager. Responsibility for the management and implementation of this Policy is with the Director Corporate Business. Group Leader Organisation Development. Other responsibilities are detailed within this Policy.

10 References

- *Government Information (Public Access) Act 2009* (NSW)
- *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

- **Approval date: 14/09/2017**
- **Responsible Section: N/A**
- **Superseded policies/procedures:**
- **Next review date: 14/09/2021**

Table of amendments

Amendment	Authoriser	Approval ref	Date