WORKPLACE SURVEILLANCE POLICY

Summary:
The purpose of this policy is to provide clear direction on the application of the *NSW Workplace Surveillance Act 2005* at Tenterfield Shire Council.

Policy Number	3.231
File Number	N/A
Document version	V1.0
Adoption Date	24 February 2021
Approved By	Council
Endorsed By	Council
Minute Number	25/21
Consultation Period	N/A
Review Due Date	February 2024 – 3 years
Department	Office of Chief Corporate
Policy Custodian	Manager Finance & Technology
Superseded Documents	Nil.
Related Legislation	Privacy and Personal Information Protection (PPIP) Act 1998 Government Information (Public Access) (GIPA) Act 2009 Local Government (LG) Act 1993 Protection of the Environment Operations (POEO) Act 1997 Workplace Surveillance (WS) Act 2005 Surveillance Devices (SD) Act 2007 Road Rules (RR) 2008 Environmental Planning and Assessment (EP&A) Act 1979 Evidence Act 1990 (EA) State Records Act 1998
Delegations of Authority	Manager Finance & Technology

1. Overview

This policy outlines the requirements of the NSW Workplace Surveillance Act 2005 and how workplace surveillance will operate under this Act at Tenterfield Shire Council.

2. Policy Principles

The workplace surveillance policy will be operated fairly, within applicable legislative requirements and only for the purposes for which it is established in the policy or which are subsequently agreed in accordance with this policy.

The surveillance devices will be operated with due regard to the privacy and civil liberties of individual members of the public, including the rights to freedom of religious and political expression and assembly.

Access to the surveillance monitoring equipment shall be restricted to authorised staff and will be protected from unauthorised access.

3. Policy Objectives

The objective of this policy is to ensure that Council complies with the requirements of the Workplace Surveillance Act 2005 and represents formal notification to all Council employees, councillors, contractors and volunteers, at all Council sites and premises about activities that fall within the statutory definitions of surveillance.

The use of certain surveillance devices has the potential to deter vandalism or personal attack and is identified to reduce the safety risks associated with employees, councillors, contractors, volunteers, customers and others in the workplace and council premises. The use of certain surveillance devices will be used optimise performance, improve efficiency and improve customer service.

While Council does not intend to use surveillance methods or data to monitor staff movements, it may from time to time, or with cause, access surveillance systems and data records in order to investigate complaints or conduct other workplace investigations as appropriate.

The main objectives are to:

- Deter vandalism and/or a possible physical/verbal assault
- Reduce the safety risks associated with workers, customers and others in the workplace
- Optimise efficiency and customer service
- Identify the geographical location of employees, councillors, contractors, volunteers in the event of an emergency
- Provide data and information to defend staff against incorrect allegations
- Increase information available when conducting investigations (e.g. code of conduct and fraud related complaints, defending Council)

4. Policy Statement

Who this Policy applies to

This Policy applies to all Council employees, councillors, contractors and volunteers, at all Council sites and premises.

Workplace Surveillance
The *NSW Workplace Surveillance Act 2005* (the 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.

Notice of surveillance
This Policy is the written notification to Council employees regarding Council's activities that fall within the statutory definitions of surveillance. A copy of this policy will be provided to all staff on initial adoption and included in the induction package for new staff. Updates to this Policy will be notified to all staff.

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

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. customer service areas). As these spaces are also workplaces, the 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 installs surveillance cameras in and near worksites, plant and fleet to monitor security.

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.

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 Communication Technology logs, backups and archives
- records from Multi Function Devices

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

Council will not carry out computer surveillance of a particular employee unless it is carried out in accordance with this Policy and authorised by the Chief Executive Officer, Chief Corporate Officer, Manager Infrastructure or Manager Finance & Technology.

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 content
- 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.

Council reserves the right to access and provide access to other authorised staff members, the emails of staff who have left the organisation for the purpose of ensuring records have been kept appropriately and for continuing business operations.

The Manager Finance & Technology 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 policy and/or procedures on IT use.

Tracking surveillance
Council may use 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 or those devices under Council's BYOD Policy.

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

- monitoring performance data for maintenance and repair requirements
- knowing the location of plant, fleet and staff for Work Health and Safety or Disaster/Emergency Management purposes
- identifying opportunities for improving efficiencies in work practices
- identifying staff, plant and fleet locations to respond to emergencies
- investigations due to complaints and incidents

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.

The Chief Executive Officer delegates to the Chief Corporate Officer, Director Infrastructure and Manager Finance & Technology responsibility for access and use of data collected via tracking surveillance carried out in accordance with this section and other staff members may only access or use this data for any purpose with the express written consent of one of these delegates.

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.

Infrastructure Construction and Maintenance plant and fleet
Operational Plant and Fleet tracking data may only be accessed by staff with delegated authority from either the Chief Corporate Officer, Director Infrastructure or Manager Finance & Technology. If authorised, persons may monitor such data

in real time only for the purposes of Work Health and Safety or Disaster/Emergency Management.

Further, authorised staff (to be clear, staff with express written consent from the Chief Executive Officer, Chief Corporate Officer, Director Infrastructure or Manager Finance & Technology) will have access to Plant and Fleet performance and usage data, collected via tracking surveillance, in order to assist in prioritising and scheduling maintenance and repair to improve efficiency and maintenance management purposes.

Private and Non Private Use of Council Vehicles
Private and Non Private use of vehicles may be recorded and used for the purpose of accurately calculating Fringe Benefits Tax. Authorised staff (to be clear, staff with express written consent from the Chief Executive Officer, Chief Corporate Officer, Director Infrastructure or Manager Finance & Technology) will be provided with this data for the purpose of calculating Fringe Benefits Tax.

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 while 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.
- An alarm is activated.
- A portable radio panic button is activated.
- An emergency situation requires the ability to locate council vehicles.

How the surveillance will be carried out
Surveillance will be carried out in accordance with this Policy.

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.

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 Act and this Policy. To be clear though, staff with private leaseback arrangements and indeed all staff with Council vehicles will not be monitored in real time while not at work (ie a person won't be sitting at a screen on the weekend saying look where employee x is. If they did this would be against Council's code of conduct and the employee would face disciplinary action.) Staff with home to work use only of council vehicles may however be audited to ensure compliance with the home

to work use only requirement and if a leaseback vehicle was involved in an accident on the weekend of course Council would review the data available – the vehicle is after all still a Council asset.

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

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 Act and this Policy.

Prohibited Surveillance
Council will not, in accordance with the WS Act:

- Conduct surveillance of change rooms and bathrooms
- Use work surveillance devices for the purpose of tracking location 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 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)).*

Audit of Surveillance Methods
On an adhoc basis but at least once per annum, the Manager Finance and Technology will conduct an audit to ensure that only authorised staff have accessed the various surveillance systems in use by council:

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

And that such use has been for a purpose as outlined in this Policy.

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 Act.

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.*

Disciplinary action under Council's Code of Conduct will be taken if this policy is breached and this could lead to dismissal. To be clear Council does not condone the use of surveillance data for anything other than legitimate purposes as per this Policy. (Please refer to the Policy Breach section below).

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

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.

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.

5. Scope
This policy extends to all staff, councillors, contractors and volunteers of Council.

6. Accountability, Roles & Responsibility
All staff, councillors, volunteers and contractors are responsible for complying with this Policy.

7. 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.

8. Related Documents, Standards & Guidelines

- Tenterfield Shire Council Code of Conduct
- Privacy and Personal Information Protection (PPIP) Act 1998
- Government Information (Public Access) (GIPA) Act 2009
- Local Government (LG) Act 1993
- Protection of the Environment Operations (POEO) Act 1997
- Workplace Surveillance (WS) Act 2005
- Surveillance Devices (SD) Act 2007
- Road Rules (RR) 2008
- Environmental Planning and Assessment (EP&A) Act 1979
- Evidence Act 1990 (EA)
- State Records Act 1998

9. Version Control & Change History

Version	Date	Modified by	Details
V1.0	24/02/21	Council	Adoption of Original Policy (Res No. 25/21)