


<b>ROUS WATER POLICY</b>	Workplace Surveillance		
<b>OVERVIEW</b>	To set out the requirements for the management and use of workplace surveillance.		
<b>AUTHORISED BY COUNCIL</b>	ROUS	RRCC	FNCW
	17/06/2015	22/06/2015	22/06/2015
<b>REVIEW DATE</b>	2 years		
<b>FILE</b>	172	843	1294

## BACKGROUND

Workplace surveillance technology is used by Council as a business tool to support the delivery of its Integrated Planning and Reporting objectives.

### COMMITMENT TO COMPLIANCE

This Policy must be read in conjunction with the [Workplace Surveillance Act 2005](#) ('the Act'). The following symbol is used throughout the Policy to direct the reader to the relevant corresponding sections within the Act: 

Council is committed to compliance with all statutory requirements relating to the operation and administration of its workplace surveillance program. **This Policy is not intended to alter Council's obligations under the Act.**

### PROHIBITED SURVEILLANCE

Surveillance of an employee will not be carried out in any change room, toilet facility, shower or lunchroom at a workplace.

Surveillance of an employee using **a work surveillance device** will not be carried out when the employee is not at work. The exception is if the surveillance is computer surveillance of the use by the employee of equipment or resources (including but not limited to telephones) provided by or at Council's expense.

A **work surveillance device** is a device used for surveillance of the employee when at work for Council.

 for more information on prohibited surveillance refer to sections 15, 16, 17 and 18 of the Act.

### WORKPLACE SURVEILLANCE PROGRAM

Council's 'Workplace Surveillance Program' is a general term used to refer to anything related to or connected with undertaking workplace surveillance including but not limited to Council's Workplace Surveillance Policy, Workplace Surveillance Procedure and any supporting equipment, technology and records.

Secretarial use only		V1.0 17/06/2015
Rous Policy	RRCC Policy	FNCW Policy
Authorised Council: 17/06/2015	Authorised Council: 22/06/2015	Authorised Council: 22/06/2015

## POLICY

- 1.1 Council has a workplace surveillance program whereby surveillance of employees is carried out while they are at work.
- 1.2 An employee is **at work** for an employer when the employee is:
- 1.2.1 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
  - 1.2.2 At any other place while performing work for the employer (or a related corporation of the employer).



↑ for more information on points 1.2 - 1.2.2 refer to section 5 of the Act.



- 1.3 The objectives of Council's workplace surveillance program are as follows:
- 1.3.1 Provide for worker safety.
  - 1.3.2 Protection of Council assets.
  - 1.3.3 Budget management.
  - 1.3.4 Operational management and performance in:
    - 1.3.4.1 Asset operation, maintenance and renewal including plant utilisation.
    - 1.3.4.2 Environmental impact of activities.
    - 1.3.4.3 Service delivery including complaints.
  - 1.3.5 Corruption minimisation.
  - 1.3.6 Claims management.

### Types of surveillance

- 1.4 Surveillance of an employee means surveillance of an employee by any of the following means:
- 1.4.1 **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,
  - 1.4.2 **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),


Secretarial use only		V1.0 17/06/2015
Rous Policy	RRCC Policy	FNCW Policy
Authorised Council: 17/06/2015	Authorised Council: 22/06/2015	Authorised Council: 22/06/2015

- 1.4.3 **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).
- 1.5 Devices often have the functionality to be camera, computer and tracking surveillance devices at the same time.
- 1.6 Surveillance is not:
- 1.6.1 Health monitoring undertaken in connection with Council's health monitoring program; or
  - 1.6.2 Drug and alcohol testing undertaken in connection with Council's drug and alcohol testing program; or
  - 1.6.3 Surveillance by means of a listening device.

  for more information on points 1.4 – 1.6.3 refer to section 3 of the Act.

## Notice of surveillance

- 1.7 The Act provides that an employer has certain obligations to notify an employee about surveillance of the employee. This obligation extends to notifying casual, temporary, agency/labour hire workers, volunteers and contractors.
- 1.8 Notice to employees will be provided in accordance with the requirements of the Act:
- 1.8.1 Existing employees: written notice will be provided at least 14 days before surveillance commences.
  - 1.8.2 New employees: written notice will be provided before the employee starts work, for example, as part of the recruitment and induction process.
- 1.9 The notice will indicate:
- 1.9.1 The kind of surveillance to be carried out (camera, computer or tracking), and
  - 1.9.2 How the surveillance will be carried out, and
  - 1.9.3 When the surveillance will start, and
  - 1.9.4 Whether the surveillance will be continuous or intermittent, and
  - 1.9.5 Whether the surveillance will be for a specified limited period or ongoing.

  for more information on points 1.7 – 1.9.5 refer to section 10 of the Act.

Secretarial use only		V1.0 17/06/2015
Rous Policy	RRCC Policy	FNCW Policy
Authorised Council: 17/06/2015	Authorised Council: 22/06/2015	Authorised Council: 22/06/2015

## Additional requirements for camera, computer and tracking surveillance

- 1.10 Council will adhere to additional requirements in relation to camera, computer and tracking surveillance as required under the Act.



↑ for more information on point 1.10 refer to section 11, 12 and 13 of the Act.

## Policy on computer surveillance

- 1.11 Council will not carry out computer surveillance of an employee unless:

1.11.1 The surveillance is carried out in accordance with this Policy, and

1.11.2 The employee has been notified in advance of its Policy in such a way that it is reasonable to assume that the employee is aware of and understands the Policy.



↑ for more information on points 1.11 – 1.11.2 refer to section 12 of the Act.

- 1.12 For the purposes of clause 1.11 above and section 12 of the Act, this Policy, in conjunction with Council's Code of Conduct, Values statement, ICT Policy and ICT Procedure, constitutes Council's policy on computer surveillance of employees at work.

- 1.13 Electronic devices can be manually set up to log information. However many devices purchased 'off the shelf' are already configured by manufacturers to automatically log certain information.

- 1.14 The type of information logged will depend on the device. Some examples of the types of information that may be logged by a work surveillance device (whether through the manual set up of a device or as a standard feature) are:

1.14.1 Computer: logon/logoff; startup/shutdown; idle time; keystrokes; emails; internet usage; images/video; pictures taken; sound.

1.14.2 Telephone: calls made/received; data sent/received; images/video; pictures taken; sound; apps; emails; internet usage.

1.14.3 Security systems: arm/disarm; PIN codes panel use.

1.14.4 Motor vehicles/fleet: start/stop; idle time; speed; location.

**Note:** Any information logged, via any device, will be date and time stamped.

Secretarial use only		V1.0 17/06/2015
Rous Policy	RRCC Policy	FNCW Policy
Authorised Council: 17/06/2015	Authorised Council: 22/06/2015	Authorised Council: 22/06/2015

- 1.15 All emails whether incoming or outgoing, are subject to monitoring on a continuous basis, with random content reviews by the IT team. An email gateway is in place to scan every incoming and outgoing message for malicious code such as viruses and Trojans, for inappropriate content, for spam, for unacceptably large attachments, and for executable code that may damage Council information systems. Due to the automated nature of this process, circumstances will occur whereby legitimate email messages may be blocked in error.
- 1.16 In these instances, where appropriate, a notification is sent to both the sender and the intended recipient if an email is blocked by the email gateway. The exception to this rule is in the case of spam mail being blocked by the email gateway, in which case no notification is sent. Notifications are currently sent when emails containing potentially malicious code are received however this notification service may be suspended during times of high virus load.
- 1.17 All internet traffic is constantly monitored, sites visited are recorded continuously, and all content is scanned for malicious code and blocked where appropriate.
- 1.18 Access to certain websites is blocked completely. These sites are typically those that are popular sites with no relationship to Council business. It is Council policy to prevent access to a website if:
- 1.18.1 Accessing the website might result in an unauthorised interference with, damage to or operation of a computer or computer network operated by Council or of any program run by or data stored on such a computer or computer network, or
- 1.18.2 The website would be regarded by reasonable persons as being, in all the circumstances, menacing, harassing or offensive.
- 1.19 By logging in to Council information systems, staff accept and agree to abide by the conditions outlined in this Policy as well as Council's Code of Conduct and other policy and procedure.



**Paragraphs 1.15 – 1.19 also apply in terms of internet use.**

## Key roles and responsibilities

### 1.20 General Manager and Executive Team:

- 1.20.1 Ensure effective implementation of the Policy within their areas of responsibility.
- 1.20.2 Ensure adequate controls are implemented and maintained to safeguard privacy.
- 1.20.3 Manage, monitor and analyse the effectiveness and operation of workplace surveillance systems.

Secretarial use only		V1.0 17/06/2015
Rous Policy	RRCC Policy	FNCW Policy
Authorised Council: 17/06/2015	Authorised Council: 22/06/2015	Authorised Council: 22/06/2015

**1.21 General Manager's nominee:**

1.21.1 Oversee the operation of the Policy.

1.21.2 Administer Council's workplace surveillance program.

**1.22 Employees:**

1.22.1 Report their own personal misconduct and the misconduct of others. Such reports can be made directly to the employee's supervisor/ manager, as a Code of Conduct complaint, or as a Public Interest Disclosure using Council's Public Interest Disclosure Policy.

**1.23 Supervisors:**

1.23.1 Ensure compliance with the requirements of the *Workplace Surveillance Act 2005* with respect to notice of surveillance to agency/labour hire workers, volunteers and contractors.

**1.24 Managers:**

1.24.1 Ensure compliance with the requirements of the *Workplace Surveillance Act 2005* with respect to notice of surveillance to agency/labour hire workers, volunteers and contractors.

1.24.2 Manage, monitor and analyse the effectiveness and operation of workplace surveillance systems.

1.24.3 Managers who are responsible for assets and sites must ensure that Council remains compliant with the *Workplace Surveillance Act 2005* with regard to camera surveillance at those sites. This includes:

1.24.3.1 Ensuring camera casing or other equipment that would clearly indicate the presence of a camera are clearly visible in the place where the surveillance is taking place; and

1.24.3.2 Ensuring signs notifying people that they may be under surveillance are clearly visible at the entry points to those places.

**1.25 IT team:**

1.25.1 Maintain and ensure the security and integrity of surveillance systems and surveillance information.

1.25.2 Undertake email and internet content/usage reviews.

1.25.3 Coordinate and administer the installation, removal and replacement of tracking surveillance for software and hardware.

1.25.4 Meet the requirements of the *Workplace Surveillance Act 2005* when installing camera surveillance equipment. This includes:

Secretarial use only		V1.0 17/06/2015
Rous Policy	RRCC Policy	FNCW Policy
Authorised Council: 17/06/2015	Authorised Council: 22/06/2015	Authorised Council: 22/06/2015

1.25.4.1 Ensuring camera casing or other equipment that would generally indicate the presence of a camera are clearly visible in the place where the surveillance is taking place; and

1.25.4.2 Ensuring signs notifying people that they may be under surveillance are clearly visible at the entry points to those places.

**1.26 Purchasing and Fleet Officer:**

1.26.1 Coordinate and administer the installation, removal and replacement of tracking surveillance for all plant and motor vehicles. This includes compliance with the requirements of the *Workplace Surveillance Act 2005* with respect to, for example, the display of a notice about the use of tracking surveillance.

1.26.2 Monitor and analyse mileage, fuel use and other data for the purpose of optimising plant and motor vehicle performance.

**1.27 Human Resources team:**

1.27.1 Ensure compliance with the requirements of the *Workplace Surveillance Act 2005* with respect to notice of surveillance to employees.

1.27.2 Support and guide supervisors and managers to ensure compliance with the requirements of the *Workplace Surveillance Act 2005* with respect to notice for agency/labour hire workers and volunteers.

**Access to, use, disclosure, storage and retention of surveillance information**

1.28 Surveillance information means information obtained, recorded, monitored or observed as a consequence of surveillance of an employee.

1.29 Council acknowledges the need to ensure that effective controls are implemented and maintained in relation to the access, use, disclosure, storage and retention of surveillance information that is personal information.

1.30 Personal information will be managed in accordance with Council's Privacy Management Policy and the *Privacy and Personal Information Protection Act 1998*. A person about whom surveillance information has been collected has a right to access that information, as does their direct Supervisor, Manager, Director and the General Manager.

1.31 The General Manager may grant access to surveillance information to any person but only as permitted under Council's Privacy Management Policy, any relevant Code of Practice and the *Privacy and Personal Information Protection Act 1998*. This includes granting access for the purpose of seeking advice or undertaking an investigation.

Secretarial use only		V1.0 17/06/2015
Rous Policy	RRCC Policy	FNCW Policy
Authorised Council: 17/06/2015	Authorised Council: 22/06/2015	Authorised Council: 22/06/2015

- 1.32 Any person that has access to surveillance information must ensure the confidentiality of the information they have access to and will be required to sign a confidentiality agreement. They are not permitted to and must not disclose or discuss any information or event with any person not directly involved with or permitted to access surveillance information. This includes not disclosing information to family, friends or other third parties.
- 1.33 In accordance with the *Privacy and Personal Information Protection Act 1998* ('PPIP Act') and Council's Privacy Management Policy, employees who intentionally disclose personal information received in relation to this workplace surveillance program to an unauthorised person are in breach of the PPIP Act and the Privacy Management Policy.

#### **Misconduct detected/confirmed through use of surveillance**

- 1.34 Non-compliance with Council Policy, Procedure, misuse of Council property or misconduct detected through the use of surveillance will be dealt with in accordance with the disciplinary procedures of the Local Government (State) Award.

#### **Review of Policy**

- 1.35 A review of this Policy will be undertaken at least every two years to ensure consistency with the requirements of the *Workplace Surveillance Act 2005*, to determine whether the objectives of the workplace surveillance program remain valid and whether the Policy remains appropriate for achieving those objectives.

#### **PROCEDURES**

PROCEDURE: Workplace Surveillance.

#### **RELATED PROCEDURES**

PROCEDURE: Motor Vehicles Conditions of use for Road Registered Motor Vehicles.

#### **LEGISLATION**

*Independent Commission Against Corruption Act 1988.*

*Public Interest Disclosures Act 1994.*

*Privacy and Personal Information Protection Act 1998.*

*State Records Act 1998.*

*Work Health and Safety Act 2011.*

*Workplace Surveillance Act 2005.*

#### **RELATED DOCUMENTS**

Code of Conduct.

Code of Conduct Procedures.

ICT Agreement.

Procurement Policy.

Public Interest Disclosures Policy.

Privacy Management Policy.

Values statement.

Work Health and Safety Management System.

#### **CONTACT OFFICER**

General Manager.

Secretarial use only		V1.0 17/06/2015
Rous Policy	RRCC Policy	FNCW Policy
Authorised Council: 17/06/2015	Authorised Council: 22/06/2015	Authorised Council: 22/06/2015