KEMPSEY SHIRE COUNCIL

WORKPLACE SURVEILLANCE **5.5.57**

Policy No. and Title	5.5	Conditions of Employment Policy
Procedure	5.5.57	Workplace Surveillance
Version	5	
Date Adopted	21 September 2016	

1 PURPOSE AND CONTEXT

a) The purpose of this procedure is to ensure that the Council complies with the requirements of the Workplace Surveillance Act 2005 and Surveillance Devices Act 2007. The procedure does not provide for, or signal any changes, to the practices of the Council. However, the Workplace Surveillance Act requires that employees be formally notified of any actions by the Council that would fall within the definitions of surveillance.

b) The Work Place Surveillance Act deals with surveillance of employees by means of cameras, computers or tracking devices and requires that employees are notified as to the nature of that surveillance. The notice provided to staff must indicate:

i) The kind of surveillance to be carried out (camera, computer or tracking).

ii) How the surveillance will be carried out.

iii) When the surveillance will start.

iv) Whether the surveillance will be continuous or intermittent.

v) Whether the surveillance will be for a specified limited period or ongoing.

c) The Surveillance Devices Act prohibits a person to:

i) Knowingly install, use or cause to be used or maintain a listening device.

ii) Overhear, record, monitor or listen to a private conversation to which the person is not a party, or

iii) Record a private conversation to which the person is a party.

d) Any surveillance type activity that is undertaken by the Council must be in accordance with the Acts and specifically the notice provided to employees. Any surveillance outside the parameters of the notice is considered to be covert surveillance and must be authorised by a Magistrate.

2 DEFINITIONS

a) Under the Workplace Surveillance Act 2005, surveillance of an employee means surveillance of an employee by any of the following means:

i) 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.

ii) 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).

iii) 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).

3 STATEMENT

a) The Council is committed to meeting its statutory obligations under the Workplace Surveillance Act 2005, Surveillance Devices Act 2007 and this Procedure in conjunction with the Internet, Intranet and Email Acceptable Use Procedure (5.10.1) and represents the formal notification to employees about activities of the Council that fall within the statutory definitions of surveillance.

b) The Schedules to this procedure detail instances of activity by the Council that are covered by the surveillance provisions, being: camera surveillance; computer surveillance; and tracking surveillance.

c) The Council will also comply with the legal requirements of the Acts where surveillance is prohibited. These are contained in Part 3 of the Work Place Surveillance Act (Sections 15 to 18) and cover:

i) A prohibition on surveillance in any change room, toilet facility, shower or other bathing facility at the workplace.

ii) A prohibition on surveillance when the employee is not at work except in cases of computer surveillance where the employee is using equipment and/or resources supplied by the Council. If staff connects to the Council via a private computer, such surveillance shall be restricted to Council equipment only.

iii) A prohibition on blocking the delivery of emails unless notice (prevented delivery notice) has been given to the employee or where the incoming communication is perceived to be spam or a threat to the security of the Council's systems or contains potentially menacing, harassing or offensive material.

iv) A prohibition on preventing delivery of an email or access to a website merely because it has been sent by or on behalf of an industrial organisation of employees or contains information about industrial matters.

d) This procedure will be emailed to all employees and posted to employees who do not have email accounts. It will also be attached to pay slips of all employees. It will be published on the Council's web site.

e) The procedure will be provided by Human Resources to all new staff prior to their undertaking employment with the Council.

f) This procedure will be reviewed annually or as dictated by legislative or other regulatory requirements.

VARIATION

Council reserves the right to review, vary or revoke this procedure which will be reviewed periodically to ensure it is relevant and appropriate.

Workplace Surveillance Procedure Schedule

Schedule A – Camera Surveillance

Security Cameras

The Council operates surveillance cameras on the outside of buildings or structures for the purpose of ensuring the safety and security of staff, visitors and the Council's premises and facilities at the following locations:

- Thompson Street Depot.
- Crescent Head Landfill site.
- Civic Centre Car Park.
- Customer Service Centre.
- South West Rocks Transfer Station.
- West Kempsey Sewage Treatment Plant
- South West Rocks Sewage Treatment Plant
- South West Rocks Water Recycling Plant
- Sherwood Bridge
- Kempsey Saleyards

The Council operates surveillance cameras on the inside of buildings for the purpose of the security of goods and equipment at the following locations:

- Thompson Street Depot Workshop (caged area near the doorway between the store and workshop)
- Thompson Street Depot (Server Room)
- Administration Building, 22 Tozer Street, West Kempsey (Server Room)

The Council operates surveillance cameras on the outside of buildings for the purpose of improving community safety and reducing antisocial activity in the Kempsey CBD at the following locations:

- Clyde Street (from Belgrave Street to Forth Street)
- Savages Lane
- Clyde Street Car Park
- Belgrave Street (between Kempsey Hotel and the end of the Aldi Complex, and across to John Street)

Cameras are used for the surveillance of persons and camera footage may be accessed and used as evidence where an act (e.g. theft, assault of a person, damage to facilities) has occurred that warrants investigation by the Council. Such records may also be required by law to be provided to a member or officer of a law enforcement agency or a Court for use in connection with the detection, investigation or prosecution of an offence.

Notices that a Council premise is monitored by cameras are located at each of the entrances at the following locations:

- Thompson Street Depot.
- Crescent Head Landfill site.
- West Kempsey Sewage Treatment Plant.

Surveillance cameras are located in and around facilities requiring monitoring for the safety or security of individuals or property and are not disguised or secreted.

Security cameras are in place as at the date of approval and promulgation of this procedure. Camera security monitoring is continuous and ongoing.

Mobile Telephone Cameras

Cameras in mobile telephones supplied by the Council are not to be used to record images of any persons without their knowledge or consent.

Schedule B – Computer Surveillance

General Use of Council Information Technology Systems and Facilities

Use of the Council's computers and associated systems is governed by the Internet, Intranet and Email Acceptable Use Procedure (5.10.1).

This procedure prescribes the conditions under which employee's access is provided to the Council's Information Technology facilities and systems. The policies also cover contractors and volunteer users.

In accordance with that procedure, authorised staff of the IT Unit, or other authorised personnel may access Council computers, computer logs and other system records, databases and backups to ensure the security, confidentiality, availability and integrity of Council IT systems.

From time to time the Council may investigate alleged breaches of the law or Council policies by staff using its IT systems and facilities and this can involve accessing the staff member's computer and electronic records. For staff, such investigations may involve misconduct or serious misconduct and are managed in accordance with the provisions of the Council's Disciplinary and Fair Treatment Procedure (5.5.11).

The Council monitor's staffs use of Council computers and IT systems in the following areas:

a) Council workstations, servers, email and network services, printers, network connected devices, and connections to the internet.

b) The Council retains logs, backups and archives of computing activities, which may be audited. Such records are the property of the Council, are subject to State and Federal laws and may be used as evidence.

c) Monitoring may include, but is not limited to; storage volumes download volumes, breaches of intellectual property laws, suspected malicious code or viruses.

Computer surveillance is intermittent but ongoing and is in place as at the date of approval and promulgation of this procedure.

Email and Internet

Council's Internet, Intranet and Email Acceptable Use Procedure (5.10.1) forms part of this notice to staff.

Email of staff members is not routinely read or monitored. However, emails are records of the Council and should be managed accordingly and will be accessible in that context. An email may also be the subject of an application under GIPA or privacy legislation.

The Council may access and monitor staff use of the Council email and internet systems in the following ways:

a) The Council monitors email server performance and retains logs, backups and archives of emails sent and received through the Council server.

   Even where the user has deleted an email, the Council may still retain archived and/or backup copies of the email. Only staff authorised by the General Manager may examine such records.

b) The Council retains logs, backups and archives of all internet access and network usage. These records may be audited, are subject to State and Federal laws and may

be used as evidence. While individual usage is not routinely monitored, unusual or high volume activities may warrant more detailed examination.

c) For the purposes of producing the email in response to a legal requirement or other lawful investigation;

d) For the purpose of determining, as part of an investigation by the Council, whether there has been unacceptable use of email to abuse or harass other persons.

e) For the purpose of determining whether there has been a breach of the Council's policies and procedures in the use by the staff member of the Council's resources to access the internet.

f) For the purpose of investigating allegations of misconduct or to provide materials to external investigative authorities lawfully investigating possible criminal conduct.

Specific provisions related to access to email messages held on the Council's servers are contained in the Internet, Intranet and Email Acceptable Use Procedure.

Email and Internet surveillance is intermittent but ongoing and is in place as at the date of approval and promulgation of this procedure.

Schedule C – Tracking Surveillance

The Council currently operates Global Positioning System tracking devices located in Plant items: The Plant items include Backhoes and Graders configured with a system that tracks hours meter readings, location of machine and machine health via the internet.

The purpose of such tracking devices is primarily used to monitor machine health and could be used to monitor the location of staff.

Other Items

Council may also gather information relating to staff through:

Security Alarm and Swipe Card Access Systems

For security purposes, when a staff member arms or disarms an alarm system throughout Council's premises either through entering their security access code or using swipe card technology, their security code number is recorded in a computer database at our monitoring company.

The Council may access and monitor staff use of the Security Alarm and Swipe Card Access systems in the following ways:

a) For the purpose of ensuring security at our workplace and is an ongoing process.

b) For the purposes of producing the security access code records in response to a legal requirement or other lawful investigation.

c) For the purpose of determining, as part of an investigation by the Council, whether there has been unacceptable access to premises.

d) For the purpose that is directly or indirectly related to taking disciplinary action or legal proceedings against an employee as a consequence or any alleged unlawful activity while at work for Council.

e) For the purpose of determining whether there has been a breach of the Council's policies in the use by the staff member of the Council's resources to access premises.

f) For the purpose of investigating allegations of misconduct or to provide materials to external investigative authorities lawfully investigating possible criminal conduct.

Information gathered may be made available to a member or officer of a law enforcement agency or a Court for use in connection with the detection, investigation or prosecution of an offence.

Security Alarm and Swipe Card Access Systems surveillance is ongoing and is in place as at the date of approval and promulgation of this procedure.