

Workplace Surveillance Policy

Policy Type: Operational Policy Policy Owner: Chief Executive Officer	Policy No.: OP- 037 Last Review Date: 29 March 2019
--	--

Policy Objectives

The objective of this policy is to detail an effective, accountable and transparent framework for managing workplace surveillance that ensures compliance with relevant surveillance and privacy legislative requirements.

Policy Scope

This policy applies to all employees and is for the awareness of volunteers and contractors in City of Melville workplaces.

Policy Statement

Surveillance is utilised within the workplace to

- assist with community and employee safety
- ensure the security of assets and equipment owned and operated by City,
- assist with the planning and management of assets and equipment owned and operated by City for service delivery to ensure their efficient utilisation,
- assist with the planning and management of resourcing needs,
- assist in workplace investigations.

1. Responsibility

Chief Executive Officer

- Ensure steps are taken to deploy and communicate the Policy.

Directors, Executive Managers, Operational Managers and Supervisors

- Assist the Chief Executive Officer in the deployment and communication of the Workplace Surveillance Policy.
- Notify People Services of any non compliance with the Workplace Surveillance Policy.

Designated Officers

- Monitor, analyse and report on surveillance systems assigned to them and any non compliance with the Workplace Surveillance Policy to People Services.

Executive Manager Governance and Legal Services

- Ensure the workplace surveillance policy is compliant with surveillance and privacy legislative requirements

Employee Services Coordinator

- Coordinate investigate of reported breaches of the policy by employees;
- Report any non-compliance with the Workplace Surveillance Policy to the Chief Executive Officer.

Employees

- Report non compliance with the Workplace Surveillance Policy to their supervisor who has an obligation to report it to the Employee Services Coordinator.

2. Types of workplace surveillance

The types of workplace surveillance that the City undertakes include, the following:

- Camera surveillance – dash cameras, Go Pro cameras, Closed Circuit Television (CCTV)
- Information, Communication and Technology surveillance
 - in relation to all usage on the City's data and communications network or on City owned information technology equipment including but not limited to application usage, internet, software and email use
 - Telephone usage and location services on mobile devices
- Asset Security - Security and swipe card facilities access
- Tracking surveillance –Global Positioning System (GPS) tracking devices.

3. How the surveillance will be carried out

Surveillance will be carried out in accordance with surveillance and privacy legislative requirements.

4. Prohibited Surveillance Areas

Surveillance is prohibited in the following areas,

- change rooms,
- toilets,
- showers or bathing facilities at a workplace, and/or

any other area identified under any legislation or industrial instrument applicable to the City.

5. Recordkeeping, Confidentiality and Privacy

The City will ensure that surveillance records will at all times remain confidential and, access to such records will be in accordance the City's Records Management Policy OP-015.

The Chief Executive Officer, Executive Manager Governance and Legal Services or Executive Manager Organisational Development may authorise a designated officer to access relevant surveillance records to:

- assist with community and employee safety
- ensure the security of assets and equipment owned and operated by City,
- enable planning, management and efficient utilisation of assets and equipment owned and operated by City is achieved,
- help plan and manage resourcing needs
- assist in workplace investigations

Inappropriate use of surveillance records by any employee is deemed to be inconsistent with their obligations to the City and must be reported to the Governance & Legal Services. Tampering with or disabling surveillance equipment so that it will cease to be effective is prohibited. Such actions by any person may, following investigation, result in disciplinary action that could include termination of employment.

Policy Definitions

Camera:	An electronic device capable of monitoring or recording visual and or audio activities in the workplace.
Computer	Surveillance by means of software or other equipment that monitors or records the information input or output, or other use of a computer.
Surveillance:	Observation or monitoring by means of an electronic device such as a camera, computer, GPS system and through the electronic access points and security gateways.
Designated Officer:	Employee tasked with monitoring, analysing and reporting on monitoring and surveillance duties and equipment assigned to them.
Tracking Surveillance:	Surveillance by means of an electronic device whose primary purpose is to monitor or record geographical location or movement, such as GPS device or location services on mobile devices.
Workplace	A workplace is a place where work is carried out for a business or undertaking and includes any place where a worker goes, or is likely to be, while at work. A place can include any vehicle or plant.

Other References that may be applicable to this Policy

Legislative Requirements:

Delegated Authority:

Plan / Policy / Framework:

Procedure:

Work Instructions / Process Maps:

Forms / Supporting Documents (internal):

Supporting Documents (external):

Origin/Authority

Meeting the Policy was adopted at

Enter date of meeting here

Reviews

Enter title of reviewer here

Enter date of review here