Workplace Surveillance Policy

Table of Contents

1 Purpose

The Department of Communities and Justice (the department) is committed to protecting the health, safety, and wellbeing of employees, clients and visitors, along with critical information and assets. Workplace monitoring and surveillance commonly occurs across NSW workplaces and supports the provision of a safe working environment by improving security – improved security results in a safer workplace.

The purpose of this policy is to describe the circumstances in which the department may conduct surveillance of its employees. The policy ensures consistency, equity, and accountability in the implementation, application, and management of workplace surveillance across the department.

The *Workplace Surveillance Act 2005* (NSW) regulates surveillance of employees at work by means of camera, computer, and tracking devices, and requires that employees be notified as to the nature of that surveillance.

2 Definitions

For the purposes of this policy the following terms and definitions apply:

Term	Definition
Act	Means the *Workplace Surveillance Act 2005* (NSW)
At work	Includes: • where the employee is at a department premises whether or not they are performing work at the time; • operating a department owned and/or leased mobile asset, including a vehicle; and • at any other place while performing work for the department.
Department	Means the Department of Communities and Justice (DCJ)
Departmental Communications Device (DCD)	A device provided by the department, which is capable of receiving or transmitting telephone communications, electronic data, email, text messages, videos, or photos, internet access including cellular/satellite telephones, pagers, personal handheld computers (PDAs) and mobile duress alarms.
Employee / staff	Means current employees, contractors, consultants, and volunteers who have access to any department premises,

Term	Definition
	equipment, or systems, including IT Resources, adjuncts, and conjoins.
Workplace	Means any department premises, or any other place where employees work (including working from home), or any part of such premises or place where work is carried out, including any place where an employee goes, or is likely to be, while at work for the department.

3 Scope

This policy applies to current employees, contractors, consultants, and volunteers who have access to any department premises, equipment, or systems, including IT resources and networks.

Third parties such as judicial officers and members are out of scope.

The policy is to be referred to in the absence of a business area having an existing surveillance policy consistent with the requirements of the Act (e.g. Office of the Sheriff NSW, CSNSW, YJ).

4 Policy statement

The activities of staff may be monitored while at work. Monitoring of staff activities is conducted by the department in accordance with the Act. The department carries out surveillance in the form of monitoring for reasons including to ensure:

- the health, safety and welfare of employees, students and visitors, for example, by installing fixed cameras in places of work;
- the integrity, security and service delivery of its systems and networks;
- the protection of public revenue; and
- compliance with its legal obligations, including reporting obligations.

Monitoring may include:

- use of internet, email, network and computer facilities at the workplace, or on a DCD, or which are used at the department's expense;
- use of software applications that record and/or analyse activity including workplace location and use, logon details and times, data changes and deletions, telephone usage, audio visual links (e.g. Microsoft Teams), photocopier and printer use;

- location tracking of a DCD and department vehicle, which may be fitted with a GPS or other tracking capability device or application;
- entry, exit, and movement within workplace facilities where users have an individually allocated access card, biometric information, or key card; and
- recording of camera and video footage (e.g. CCTV, Microsoft Teams).

The department collects, and stores information obtained through surveillance monitoring (including logs, images, backups, and archives), which may be audited.

In monitoring and recording employee activities, the department must meet its obligations and responsibilities under the *Surveillance Devices Act 2007, Privacy and Personal Information Protection Act 1998*, Code of Ethical Conduct, Information Management Policy, Information Security Policy, IT Security Policy, Data Privacy and Protection Policy, IT Acceptable Use Policy, Privacy Policy and Privacy Management Plan, and the Records Management Policy.

Failure of an employee to comply with legislation, policy and associated standards and procedures may result in disciplinary action up to and including dismissal. Non-compliance may also be reported to NSW Police Force or other relevant authority if criminal activity is suspected.

5 Policy requirements

The department creates a transparent workplace surveillance environment by:

- Providing notice to staff as relevant to their workplace of the type of surveillance in place through a variety of means to meet the notice requirements of the Act, including signage, electronic notifications, and intranet communications.
- Providing clear notice of camera surveillance on department premises through appropriate signage clearly visible at each entrance to that place.
- Providing clear notice to employees about the use of tracking devices, including a notice clearly visible on the vehicle or other thing indicating that the vehicle or thing is the subject of tracking surveillance.
- Where a new surveillance activity is introduced (computer, camera or tracking surveillance), at least 14 days' notice will be provided to affected staff in writing (unless all affected employees agree to a lesser period of notice).
- Notifying prospective new staff of surveillance activity in their letter of offer and induction information prior to commencement.

- Not undertaking unlawful covert or prohibited camera surveillance (change room, toilet facility or shower or other bathing facility at a workplace).
- Only using surveillance information for a legitimate business purpose, and only using it and disclosing it as permitted by law.
- Not routinely using workplace surveillance to monitor employee performance or attendance without an established clear reason.
- Only using surveillance information in managing conduct or disciplinary matters where there is a legitimate reason and in accordance with the Act and the department's Code of Conduct.

6 When the department may conduct surveillance

The department may from time to time:

- conduct surveillance, including surveillance of individual employees; or
- access, use or disclose information or records obtained in the course of monitoring for surveillance in relation to individual employees.

The department may use or disclose surveillance information or surveillance records for purposes authorised under the Act. These purposes include:

- for the legitimate business activities or functions of the department, including internal inquiries and investigations of alleged unlawful activities or activities that are alleged to be in breach of any law, policy or code of conduct or in breach of a person's duties to the department as its employee;
- for use or disclosure in any legal proceedings (including an inquiry by the Independent Commission Against Corruption or the NSW Ombudsman) to which the department is a party or is directly involved;
- use of data including personal information for the purposes of vehicle tracking;
- disclosure to a member or officer of a law enforcement agency for use in connection with the detection, investigation or prosecution of an offence;
- where otherwise required or authorised by law to do so (for example, if the department is required to comply with a search warrant or subpoena);
- where the department considers this is reasonably necessary to avert a serious and imminent threat of:
    - serious violence to a person; or
    - damage to property (including disruption to the department's business, systems or operations).

7 Related legislation/regulation and other documents

7.1 Legislation

- *Anti-Discrimination Act 1977*
- *Court Security Act 2005*
- *Crimes Act 1900*
- *Crimes (Administration of Sentences) Regulation 2014*
- *Crimes (Domestic and Personal Violence) Act 2007*
- *Criminal Records Act 1991*
- *Drug Misuse and Trafficking Act 1985*
- *Firearms Act 1996*
- *Government Information (Public Access) Act 2009*
- *Government Sector Employment Act 2013*
- *Government Sector Employment Regulation 2014*
- *Law Enforcement (Powers and Responsibilities) Act 2002*
- *Privacy and Personal Information Protection Act 1998*
- *Privacy and Personal Information Protection Regulation 2019*
- *Sheriff Act 2005*
- *State Records Act 1998*
- *Summary Offences Act 1988*
- *Surveillance Devices Act 2007*
- *Workplace Surveillance Act 2005*

7.2 Department corporate policy

- Code of Ethical Conduct
- Data Privacy and Protection Policy
- Information Management Policy
- Information Security Policy
- IT Acceptable Use Policy
- IT Security Policy
- Privacy Policy
- Privacy Management Plan
- Records Management Policy

8 Document information

Document name	Workplace Surveillance Policy
Document reference	TBC
Replaces	Nil
Applies to	All individuals included in the scope of the policy
Policy administrator	Security Strategy and Policy Infrastructure and Assets Branch Corporate Services Division
Approval	Catherine D'Elia, Deputy Secretary Corporate Services 13/06/2024

9 Support and advice

Business unit	Security Advisory and Planning Infrastructure and Assets Branch Corporate Services Division
Email	security.advisory@dcj.nsw.gov.au

10 Version and review details

Version	Effective date	Reason for amendment	Due for review
1.0	13/06/2024	First policy	12/06/2026