

ACT Public Sector Workplace Privacy Policy

**Notice to Workers: Workplace Surveillance**

**Policy Number: xx/xxxx**

**Issue Date: [MONTH] 2024**

Issued by:

Office of Industrial Relations and Workforce Strategy

Chief Minister, Treasury and Economic Development Directorate

Contents

[Workplace Privacy Policy 1](#_Toc164767847)

[Introduction 4](#_Toc164767848)

[Objective 4](#_Toc164767849)

[Application 4](#_Toc164767850)

[Key Legislative Provisions 5](#_Toc164767851)

[Roles and Responsibilities 6](#_Toc164767852)

[Principles 7](#_Toc164767853)

[ACTPS Code of Conduct 7](#_Toc164767854)

[Record Keeping 7](#_Toc164767855)

[Human Rights 7](#_Toc164767856)

[Terminology 8](#_Toc164767857)

[Consultation 9](#_Toc164767858)

[Review 9](#_Toc164767859)

[Approval Authority 10](#_Toc164767860)

[Workplace Surveillance and Notice to Workers 11](#_Toc164767861)

[Provision of Policy and Notice to Current and New Workers 11](#_Toc164767862)

[Consultation on Changes to and Conducting of Surveillance 11](#_Toc164767863)

[Permitted Surveillance 12](#_Toc164767864)

[Data surveillance 12](#_Toc164767865)

[Kinds of data surveillance devices 12](#_Toc164767866)

[How data surveillance is conducted 12](#_Toc164767867)

[Who is regularly or ordinarily the subject of data surveillance? 14](#_Toc164767868)

[When data surveillance occurs 14](#_Toc164767869)

[Purpose for Which Data Surveillance Records May be Used or Disclosed 14](#_Toc164767870)

[Security of the Network 14](#_Toc164767871)

[Audit and Legal Requirements 14](#_Toc164767872)

[Efficiency of ACT Government Business Activities 14](#_Toc164767873)

[Optical Surveillance 14](#_Toc164767874)

[Kinds of optical surveillance 14](#_Toc164767875)

[How optical surveillance is conducted 14](#_Toc164767876)

[Who is regularly or ordinarily the subject of optical surveillance? 15](#_Toc164767877)

[When optical surveillance occurs 15](#_Toc164767878)

[Purpose for Which Optical Surveillance Records May be Used or Disclosed 15](#_Toc164767879)

[Security of Workers and Assets and Members of the Public 15](#_Toc164767880)

[Audit and Legal Requirements 15](#_Toc164767881)

[Efficiency of ACT Government Business Activities 15](#_Toc164767882)

[Tracking surveillance 16](#_Toc164767883)

[Kinds of tracking surveillance 16](#_Toc164767884)

[How tracking surveillance is conducted 16](#_Toc164767885)

[Who is regularly or ordinarily the subject of tracking surveillance? 16](#_Toc164767886)

[When tracking surveillance occurs 17](#_Toc164767887)

[Purpose for Which Tracking Surveillance Records May be Used or Disclosed 17](#_Toc164767888)

[Security of ACT Government Workers and Assets 17](#_Toc164767889)

[Audit and Legal Requirements 17](#_Toc164767890)

[Efficiency of ACT Government Business Activities 17](#_Toc164767891)

[Misconduct and Underperformance 17](#_Toc164767892)

[Covert Surveillance 17](#_Toc164767893)

[Prohibited Surveillance 18](#_Toc164767894)

[Further Information 18](#_Toc164767895)

## Introduction

1. As an employer, the ACT Public Sector (ACTPS) has a responsibility under the *[Workplace Privacy Act 2011](https://www.legislation.act.gov.au/a/2011-4)* (the WP Act) to notify its workers of the nature and purpose of workplace surveillance operating within ACTPS directorates and agencies.
2. The WP Act regulates the collection and use of workplace surveillance information. The purpose of this Policy is to ensure that all ACTPS workplaces comply with the requirements of the WP Act.

## Objective

1. This Policy represents the ACTPS requirement pursuant to section 13 of the WP Act, that formal notification be provided to workers about the workplace surveillance, including information about devices in operation, and when information from these devices can be accessed or used.

## Application

1. This Policy is a whole-of-government strategy issued by the Head of Service under section 17(2)(a) of the [*Public Sector Management Act 1994*](https://www.legislation.act.gov.au/a/1994-37/) (the PSM Act). It applies to all ACT Government directorates and public sector bodies in relation to public employees and executives employed in the ACTPS under the PSM Act, and binds all workers engaged under the PSM Act, and all public sector employers within the meaning of section 152(1)(a) of the PSM Act. For the purpose of this Policy, any reference to the Head of Service and/or Directors-General is also taken to be a reference to a public sector employer within the meaning of section 152(1) of the PSM Act.
2. Persons referred to in this Policy as workers include ACTPS employees[[1]](#footnote-1) (officers, temporary employees, casual employees, public sector members and members of the senior executive service), as well as contractors, consultants, certain students and volunteers.
3. This Policy relates to the collection and use of workplace surveillance information and workplace surveillance devices and applies to all ACTPS workers. This includes surveillance across workplaces and the use of ACT Government resources using data surveillance, optical surveillance and tracking surveillance.
4. The WP Act provides a framework for the collection and use of workplace surveillance information by Territory employers, including ACT Government directorates. The WP Act requires that workers be consulted and notified of surveillance arrangements in place in their workplaces. Consultation with workers must be undertaken at least 14 days prior to conducting any new surveillance that is not otherwise recognised in this Policy.
5. This Policy is taken to be a formal notification to ACTPS workers that surveillance arrangements are in place across all ACT Government directorates and public sector bodies. Individual directorates and public sector bodies may develop specific notifications to workers, based on operational requirements and proposed changes to existing, or new workplace surveillance.
6. This Policy is not applicable to community members within an ACTPS workplace. Community members are covered under relevant legislation and regulations, terms and conditions and signage relevant to the activity, such as notification at entrances for the use of CCTV in the area.

## Key Legislative Provisions

1. Section 7 of the WP Act identifies the meaning of a worker, being an individual who carries out work in relation to a business or undertaking, whether for reward or otherwise, under an arrangement with the person conducting the business or undertaking.
2. Section 8 of the WP Act describes an employer of a worker as a person who engages the worker to carry out work in the person’s business or undertaking. Section 9(b) of the WP Act describes a business or undertaking to include an activity conducted by a local, state or territory government.
3. Section 10 of the WP Act describes a workplace as a place where work is, has been, or is to be, carried out by, or for, someone conducting a business or undertaking. This includes where a worker is conducting work from an ACT Government building or Flexi-Space, from home under hybrid working arrangements, or an approved reasonable adjustment.
4. Section 11 of the WP Act describes surveillance as using a data, optical, or tracking surveillance device.
5. Section 13 of the WP Act requires that workers must be formally notified of surveillance arrangements in place in their workplaces. This notification **must** include:
6. the type of surveillance device in use;
7. how surveillance will be conducted;
8. who will be subject to surveillance;
9. when surveillance will be in place; and
10. the purpose(s) of surveillance.
11. The following legislation and employment frameworks are applicable to and referred to in this Policy:
* [*Workplace Privacy Act 2011*](https://www.legislation.act.gov.au/a/2011-4)*;*
* [*Information Privacy Act 2014*](https://www.legislation.act.gov.au/a/2014-24/)*;*
* [*Territory Privacy Principles (TPPs)*](https://www.oaic.gov.au/privacy/privacy-legislation/state-and-territory-privacy-legislation/territory-privacy-principles)*;*
* [*Territory Records Act 2002*](https://www.legislation.act.gov.au/a/2002-18/)*;*
* [*Work Health and Safety Act 2011*](https://www.legislation.act.gov.au/a/2011-35/)*;*
* [*Public Sector Management Act 1994*](https://www.legislation.act.gov.au/a/1994-37/)*;*
* [Public Sector Management Standards 2016](https://www.legislation.act.gov.au/di/2016-251/);
* [Public Sector Management Standards 2006](https://www.legislation.act.gov.au/di/2006-187) [repealed][[2]](#footnote-2);
* [*Listening Devices Act 1992*](https://www.legislation.act.gov.au/a/1992-57/)*;*
* [*Freedom of Information Act 2016*](https://www.legislation.act.gov.au/a/2016-55/)*;*
* [ACTPS Code of Conduct](https://www.cmtedd.act.gov.au/__data/assets/pdf_file/0018/2004921/ACTPS-Code-of-Conduct-2022.pdf);
* [*Fair Work Act 2009*](https://www.legislation.gov.au/C2009A00028/latest/text)*;*
* [Fair Work Regulations 2009;](https://www.legislation.gov.au/F2009L02356/latest/text)
* [ACTPS Enterprise Agreements;](https://www.cmtedd.act.gov.au/employment-framework/for-employees/agreements)
* [ACT Government Closed-Circuit Television Policy 2022](https://www.justice.act.gov.au/__data/assets/pdf_file/0007/2093677/Closed-Circuit-Television-CCTV-Policy.pdf);
* [Acceptable ICT Use Policy](https://www.cmtedd.act.gov.au/__data/assets/pdf_file/0006/818034/Acceptable_ICT_Use_Policy.pdf);
* [Cyber Security Policy](https://www.cmtedd.act.gov.au/__data/assets/pdf_file/0010/1900747/Cyber-Security-Policy.pdf);
* Directorate/Agency Specific Closed-Circuit Television (CCTV) Policies/Procedures; and
* Directorate/Agency Specific Information Privacy Policies.

## Roles and Responsibilities

|  |  |
| --- | --- |
| **Directors-General** | * Ensuring their workplace complies with relevant legislation, including WP Act obligations.
 |
| **Senior Executives and Executives** | * Own, oversee and accountable for surveillance devices within their area of management responsibility.
* Ensure compliance with relevant legislation, policies and procedures related to workplace privacy and surveillance devices within their division, group or branch, including maintenance of the integrity and security of the system, and the protection and interests of the public.
 |
| **Senior Executive Responsible for Business Integrity Risk (SERBIR)** | * Ensure reporting processes are in place for any breaches of this Policy.
* Investigate any reported breaches of the WP Act.
* Investigate and refer any integrity matters or Public Interest Disclosures.
 |
| **Agency Security Executive (ASE)** | * Ensure the use and disclosure of CCTV (Optical surveillance) is consistent with this Policy and any directorate or agency specific CCTV management procedures.
* Investigate any security related matters.
 |
| **ACT Cyber Security Centre** | * Conduct data surveillance, as necessary.
* Monitor the location of ACT Government ICT assets.
* Surveillance under the Acceptable ICT Use Policy.
* Investigate ICT security related matters.
* Report on ICT resource usage metrics.
 |
| **ACT Property Group** | * Ensure any surveillance conducted is compliant with this Policy.
* Ensure devices installed in ACTPS facilities are compliant with this Policy.
* Ensure no surveillance is conducted in non-work areas where possible.
 |
| **Human Resources** | * Provide support to the SERBIR.
* Ensure this Policy is made available to new staff.
 |
| **Industrial Relations and Public Sector Employment (CMTEDD)** | * The Industrial Relations and Public Sector Employment (IRPSE) branch provides advice to the whole of Government on ACTPS workplace relations matters.
* IRPSE is responsible for maintaining this Policy and ensuring it is reviewed regularly.
 |
| **Professional Standards Unit** | * The Professional Standards Unit (PSU) conducts misconduct investigations across the ACTPS under the auspices of the Public Sector Standards Commissioner and in accordance with the provisions of the relevant enterprise agreement, the PSM Act and the PSM Standards.
 |
| **WorkSafe ACT** | * WorkSafe ACT serves as the regulator under the WP Act.
* Monitor and enforce compliant with the WP Act, and by extension this Policy.
* Investigate contraventions of the WP Act.
 |
| **Workers (including Directorate staff, contractors and service providers)** | * Read this Policy.
* Understand when and how surveillance may be conducted.
* Ensure compliance with relevant legislation, policies and procedures related to workplace privacy and surveillance devices within their responsibilities.
* Report any breaches of this Policy.
 |

## Principles

1. The ACTPS is committed to fully complying with its statutory obligations under the WP Act. This Policy broadly acts as a Notice to Workers but does not represent a change in the use of surveillance across all ACTPS workplaces. However, the WP Act does regulate the use of such surveillance.
2. The ACTPS has expectations about the behaviour of its workforce. How workers undertake their work, conduct themselves with fellow workers and/or represent the ACTPS is important. It is important that workers understand their responsibilities around the use of Territory resources and property, work health safety, and behaviour, as breaching these expectations may have serious consequences.
3. Workplace surveillance is one of the systems in place that help to ensure that workers and ultimately the ACTPS are held accountable.

## ACTPS Code of Conduct

1. The ACTPS [Code of Conduct](https://www.cmtedd.act.gov.au/__data/assets/pdf_file/0018/2004921/ACTPS-Code-of-Conduct-2022.pdf) (the Code) applies to the conduct of ACTPS employees in all circumstances. The Code provides guidance on the behaviour employees should expect of themselves and their colleagues and provides guidance on behaviours that are consistent with the requirements of Section 9 of the PSM Act.

## Record Keeping

1. [*The Territory Records Act 2002*](https://www.legislation.act.gov.au/a/2002-18/) requires that information created and kept, or received and kept, as evidence and information by a person in accordance with a legal obligation, or while conducting business, must retain records, information, and data in readily accessible formats by adhering to the retention requirements outlined in records disposal schedules.
2. The Territory Records Office’s [Guidelines and Advices](https://www.territoryrecords.act.gov.au/standards) provide additional information on use and implementation of the Standard and offer opportunities to establish good practice in the records and information governance management sphere.

## Human Rights

1. The ACT is a human rights jurisdiction and all ACTPS employees are required to have regard to the [*Human Rights Act 2004*](https://www.legislation.act.gov.au/a/2004-5). Section 30 of the *Human Rights Act 2004* requires that ‘*So far as it is possible to do so consistently with its purpose, a Territory law must be interpreted in a way that is compatible with* [*human rights*’](http://www5.austlii.edu.au/au/legis/act/consol_act/hra2004148/s5.html#human_rights).
2. Section 40B of the *Human Rights Act 2004* requires a public authority to act in a way that is consistent with human rights, and when making a decision, give proper consideration to a relevant human right.

# Terminology

|  |  |
| --- | --- |
| **Business or Undertaking** | Includes a not-for-profit business; and an activity conducted by a local, state or territory government. |
| **Computer resources**  | Includes internet access and electronic communication applications. |
| **Conducts surveillance** | A person conducts surveillance if the person conducts the surveillance personally; or causes someone else to conduct the surveillance. |
| **Data Surveillance Device** | A device or program capable of being used to record or monitor the input or output of information into or from a computer but does not include optical surveillance devices. |
| **Device** | Includes an instrument, apparatus or equipment. |
| **Employer** | A person who engages the worker to carry out work in the person’s business or undertaking; and if the person who engages the worker is a corporation. Examples of an employer include but are not limited to:* principal contractor is an employer of a subcontractor; and
* host organisation is an employer of a labour hire worker.
 |
| **Human Resources** | Human Resources (HR) provides advice and support to staff, managers and executives on a variety of staffing matters, including the employment framework, performance, probation, internal reviews and complaints. HR areas across the ACTPS may have different naming conventions, such as: Employee Relations, People and Culture, People & Performance, etc. Despite these naming conventions, the fundamental purpose of HR remains the same. |
| **Misconduct** | Misconduct is defined in the relevant [Enterprise Agreement](https://www.cmtedd.act.gov.au/employment-framework/for-employees/agreements). Misconduct may include, but is not limited to, taking improper advantage of a role or information gained through a role, improperly using a Territory resource including information accessed through a role, and failing to undertake a role with reasonable care and diligence. |
| **Optical Surveillance Device** | A device capable of recording visually or observing an activity (e.g. video camera or CCTV) including a camera casing or other equipment that generally indicates the presence of an optical surveillance device but does not include spectacles, contact lenses or similar devices used by a person with impaired sight to overcome that impairment. |
| **Surveillance** | Means surveillance using a surveillance device. |
| **Surveillance Device** | A data surveillance device, an optical surveillance device or a tracking surveillance device, or a device that is combination of any two or more of these devices or a device prescribed by regulation. |
| **Tracking Device** | An electronic device capable of being used to work out or monitor the location of a person or an object or the status of an object. Examples include, but are not limited to, GPS, biometrics and radio frequency identification. |
| **Worker** | An individual who carries out work in relation to a business or undertaking, whether for reward or otherwise, under an arrangement with the person conducting the business or undertaking. Examples of a worker include but are not limited to: * an employee (including permanent, temporary, and casual employees);
* an independent contractor;
* an outworker;
* a person doing a work experience placement; and/or
* a volunteer.
 |
| **Workplace** | A place where work is, has been, or is to be, carried out by or for someone conducting a business or undertaking[[3]](#footnote-3). This may include in the home for workers with work from home arrangements. |

## Consultation

1. This Policy was consulted with the ACTPS People Forum, unions and the Office of Industrial Relations and Workforce Strategy.

## Review

1. This Policy may be reviewed from time to time and the Head of Service may vary, or revoke and substitute the Policy. Otherwise, the Policy is due for review 3 years from the last issued or reviewed date, or earlier where there are changes that affect the operation of the Policy.

|  |  |
| --- | --- |
| **Document name:** Workplace Privacy Policy 2024 (Notice to Workers: Surveillance) | **Prepared by**: Whole of Government Public Sector Employment, Office of Industrial Relations and Workforce Strategy, CMTEDD |
| **Policy Number:** xx/2024 | **Feedback to:** Whole of Government Public Sector Employment eba@act.gov.au  |
| **Issue Date:** [DATE] 2024 | **Review Date:** [DATE] 2027 |

## Approval Authority

This policy is approved by:

xxx

Deputy Director-General

Office of Industrial Relations and Workforce Strategy

Chief Minister, Treasury and Economic Development Directorate

On behalf of the Head of Service

Xx Xxxx 2024

# Workplace Surveillance and Notice to Workers

## Provision of Policy and Notice to Current and New Workers

1. This Policy will be made available to new workers prior to their commencement with the ACTPS as part of their employment offer, or contractual agreement. The Policy will also be available to all current employees (via the ACTPS Employment Portal or other means) to ensure all workers have access to it.
2. In order to meet operational requirements, individual ACT Government directorates and public sector bodies may, from time to time, require changes or the addition of new surveillance in their workplaces. Where this occurs, workers must be notified in accordance with the *Workplace Privacy Act 2011* (the WP Act) and this Policy.
3. Where there are changes or additions to whole of ACTPS workplace surveillance, this Policy will also be reissued at least 14 calendar days before surveillance starts, or for when any new surveillance activity commences that has not otherwise been described in this Policy or a period less than 14 calendar days if the affected worker(s) agrees to this.

## Consultation on Changes to and Conducting of Surveillance

1. Proposed changes to and conducting of surveillance will be consulted on in accordance with the WP Act, this Policy, as well as other related policies and legislation, and the relevant enterprise agreement.
2. Consultation with workers about how the surveillance will be conducted will be done in good faith and for no less than the required notice period of 14 calendar days before surveillance starts, or within an agreed lesser period. Under the WP Act, an employer consults with the worker in good faith if the employer gives the worker a genuine opportunity to influence the conducting of the surveillance.
3. This notification must include:
4. the kind of surveillance device to be used for the surveillance;
5. how the surveillance will be conducted;
6. who will regularly or ordinarily be the subject of the surveillance;
7. when the surveillance will start;
8. whether the surveillance will be continuous or intermittent;
9. whether the surveillance will be for a stated period or ongoing;
10. the purpose for which the employer may use and disclose surveillance records of the surveillance; and
11. that a worker may consult with the employer about the conduct of the surveillance under section 14 of the WP Act.

## Permitted Surveillance

1. Workplace surveillance is only permitted for the uses described in this Policy and may only be conducted in accordance with this Policy and in accordance with the WP Act, and only if this notice has been given to workers, except for surveillance using an optical surveillance device in a workplace.
2. The ACTPS must not conduct surveillance of a worker if they are not in a workplace, except on ACTPS provided devices and assets with tracking devices that cannot be deactivated.
3. Surveillance may be used for:
4. security and safety;
5. undertaking audit or compliance assurance reviews;
6. legal purposes, such as investigation by the PSU, ACT Policing/AFP, or the ACT Integrity Commission;
7. supporting preliminary assessments, misconduct processes, and underperformance processes; and/or
8. ensuring efficiency of activities, operations and utilisation of assets.

## Data surveillance

### Kinds of data surveillance devices

1. A data surveillance deviceis a device or program capable of being used to record or monitor the input or output of information into or from a ‘computer’ but does not include optical surveillance devices.
2. ‘Computer/s’ may include but is not limited to; ACT Government-owned or leased computers, laptops, iPad or similar tablets, docking stations, Webex or other branded smart boards, printers, soft phones, smart phones, or other network connected devices, regardless of whether the ACTPS provided device is used within a workplace, flexible workplace or home setting.
3. Future devices of another name may be introduced into the service that perform similar functions and capable of being used to record or monitor the input or output of information.
4. Software and applications used by the ACT Government are data surveillance devices under the WP Act. They log information and are required to have audit functions. These are kept and used in accordance with the [Monitoring and Logging Standard](https://actss.service-now.com/ddts?id=knwl_article_ddts&sys_id=6dbeba8b15758f80750353a7d14f1794).
5. This may also include personal (non-work provided) devices where a work-related application is used.

### How data surveillance is conducted

1. The WP Act states an employer may only conduct surveillance of a worker using a data surveillance device if:
2. the surveillance is conducted in accordance with a policy of the employer on surveillance of workers in the workplace using data surveillance devices;
3. the employer has notified the worker, before conducting the surveillance, of the policy in a way that it is reasonable to assume that the worker is aware of and understands the policy; and
4. the employer’s data surveillance policy states:
	* 1. how the employer’s computer resources may, and must not, be used;
		2. what information about the use of the employer’s computer resources is logged and who may access the logged information; and
		3. how the employer may monitor and audit a worker’s compliance with the policy.
5. In accordance with these requirements, all ICT use is monitored to detect and report inappropriate use as described in the [Acceptable ICT Use Policy](https://www.cmtedd.act.gov.au/__data/assets/pdf_file/0006/818034/Acceptable_ICT_Use_Policy.pdf), which must be provided to workers as part of the New Employee Personal Information Pack, at induction.
6. Additionally, all workers are required to acknowledge the Acceptable ICT Use Policy as part of their ACT Government network logon to government-issued computer resources, to maintain their awareness and understanding of this Policy.
7. The monitoring of ICT is also used to manage the efficiency of activities and operations such as the use of Webex or other branded smart boards in meeting rooms; the use of docking stations to indicate use of a facility or asset to optimise utilisation; or use of a printer to ensure appropriate cost distribution.
8. The monitoring of a worker’s use of ACT Government computers and ICT systems is conducted by:
9. maintaining logs, backups and archives of computing activities;
10. monitoring server performance and retention of logs, backups, and archives, including of emails sent and received through ACT Government servers;
11. requesting activity logs from service providers (e.g. Citrix, Webex smart boards);
12. retaining logs, backups and archives of all internet access and network usage;
13. applying enhanced monitoring of privileged user sessions, including session recording and command logging;
14. monitoring usage of cloud services; and
15. collecting and analysing software analytics data.
16. Even where the worker has deleted an email, the ACTPS may still retain archived and/or backup copies of the email.
17. The ACTPS may stop the delivery of an electronic communication sent to or by a worker, or stop access to a website in accordance with the Acceptable ICT Use Policy where the incoming communication or website:
18. is perceived to be spam or a threat to the security of the ACTPS or its information technology systems; or
19. contains material that might reasonably be considered to be threatening, harassing or offensive.
20. This does not include preventing delivery of an email or access to a website because it has been sent by or on behalf of an industrial association or contains information about industrial matters.
21. Records of workplace surveillance are retained in accordance with the provisions of the *Territory Records Act 2002*. Where necessary or relevant, surveillance records may be kept for a period longer than required under the *Territory Records Act 2002,* for example records may be kept until the end of legal proceedings.
22. ACT Cyber Security Centre within Digital, Data and Technology Solutions (DDTS) has access rights to all worker ICT related activity. This access is in accordance with the Acceptable ICT Use Policy. Examination of such records is only granted for purposes and to staff authorised by the relevant delegate under the Acceptable ICT Use Policy, and if in relation to a misconduct/underperformance matter in accordance with the relevant delegate under HR Delegations.
23. The ACT Integrity Commission and ACT Policing/AFP have powers represented outside of this Policy.

### Who is regularly or ordinarily the subject of data surveillance?

1. Data surveillance is applied to all workers of the ACTPS and their access to ICT systems and networks.

### When data surveillance occurs

1. Data surveillance is ongoing and may operate when the worker is using ACT Government-owned equipment and/or resources including where they are used away from the workplace (including locally or overseas). Refer to the [Overseas Working and Travel - ACT Government device and system access.](https://actss.service-now.com/ddts?id=knwl_article_ddts&sys_id=ca7524a1dbe8dd54b1744837059619a3)

# Purpose for Which Data Surveillance Records May be Used or Disclosed

### Security of the Network

1. Surveillance of ACT Government ICT systems and networks is in place to protect the efficiency, integrity, confidentiality and availability of these systems. Malicious software and viruses pose a significant risk to the ACT Government and its operations. Inappropriate use of ICT systems and networks, including internet and email, presents a risk to the integrity of the ACT Government and its processes.

### Audit and Legal Requirements

1. ICT records may be audited, are subject to Territory and Federal laws, and may be used as evidence in legal, administrative and/or disciplinary proceedings.

### Efficiency of ACT Government Business Activities

1. Data surveillance devices may be used for process control and business monitoring, such as to monitor the efficiency of use of the device and how the device may support other functions.

## Optical Surveillance

### Kinds of optical surveillance

1. An optical surveillance device is a device capable of visually recording or observing an activity. Video cameras or Closed-Circuit Television (CCTV) are examples of optical surveillance.
2. Devices including, but not limited to, body worn cameras, drones, mobile phones and dashcams may be used to capture images of workers and are considered optical surveillance devices for the purpose of this Policy.
3. Future devices of another name may be introduced into the service that perform similar functions and capable of being used to visually record or observe and activity.

### How optical surveillance is conducted

1. The WP Act states that an employer may only conduct surveillance of a worker using an optical surveillance device if:
	1. the optical surveillance device used for the surveillance is clearly visible in the workplace where the surveillance is conducted; and
	2. a sign or notice is clearly visible at each entrance to the workplace, telling people that they may be under surveillance in the workplace.
2. In accordance with these requirements, the [ACT Government Closed Circuit Television (CCTV) Policy (the CCTV Policy),](https://www.justice.act.gov.au/__data/assets/pdf_file/0007/2093677/Closed-Circuit-Television-CCTV-Policy.pdf) which governs the use of CCTV and related systems operating within ACT Government, requires that ‘*CCTV systems must be operated with proper consideration to privacy and human rights*’.
3. CCTV will not be installed in prohibited areas as defined under section 41 of the WP Act(for example toilets or change rooms, or in other locations specified under prohibited surveillancesuch asa shower or other bathing facility, a parent or nursing room, a prayer room, a sick bay, or a first-aid room).
4. Recorded images are retained and used only in accordance with the purpose for which the CCTV system was installed unless they are subject to Territory or Federal laws that may require these records to be used as evidence in legal proceedings or otherwise in accordance with the provisions of this Policy.
5. Records of workplace surveillance are retained in accordance with the requirements of the *Territory Records Act 2002*. Where necessary or relevant surveillance records may be kept for a period longer than required under the *Territory Records Act 2002*: for example, records may be kept until the end of legal proceedings.

### Who is regularly or ordinarily the subject of optical surveillance?

1. Optical surveillance is applied to Directorate workers (including contractors and service providers engaged by ACT Government directorates and public sector bodies) and members of the public.

### When optical surveillance occurs

1. Optical surveillance is ongoing. Where optical surveillance is operating in an ACT Government vehicle the optical surveillance will also operate when the vehicle is outside of the Territory.

# Purpose for Which Optical Surveillance Records May be Used or Disclosed

### Security of Workers and Assets and Members of the Public

1. Surveillance of ACT Government premises and assets is in place to ensure the security and safety of workers and assets, and for the safety and security of members of the public. Optical surveillance is used in reducing and preventing crime against property and/or persons.

### Audit and Legal Requirements

1. Optical surveillance records and images may be audited, are subject to Territory and Federal laws and may be used as evidence in legal proceedings, and administrative and/or disciplinary proceedings.

### Efficiency of ACT Government Business Activities

1. Optical surveillance systems may be used for process control and business monitoring. Including, but not limited to, public safety and events monitoring, regulatory enforcement, training and education, and parking management.

## Tracking surveillance

### Kinds of tracking surveillance

1. Tracking surveillance refers to electronic devices capable of being used to determine or monitor the location – including domestic and overseas – of a person or the status of an object.
2. Such devices may include, but are not limited to, GPS tracking devices, IP address monitoring, radio frequency identification devices, GPS tracking devices that are in ACT Government-owned and leased vehicles, and on ACT Government-owned and leased Portable Electronic Devices including mobile phones, smart phones, laptops, iPads and other devices.
3. Other examples include Corporate Cabcharge and Uber accounts that are supplied with details of user journeys; and desk booking applications such as Engage identify the location of an individual who has booked a desk.
4. Future devices of another name may be introduced into the service that perform similar functions and capable of being used to work out or monitor locations.

### How tracking surveillance is conducted

1. The Directorate may only conduct surveillance of a worker that involves the tracking of a vehicle or other thing using a tracking device if there is a notice clearly visible on the vehicle or other thing stating that the vehicle or thing is being tracked. However, in accordance with the Act, this does not apply if:
2. it is not reasonably practicable to have a notice on the vehicle or other thing; and
3. the Directorate has taken reasonable steps to notify workers that the vehicle or other thing is being tracked – for example, new users of Uber accounts are provided with information stating how their journey is tracked and why; and users of booking systems are provided with notices of use and the ability to ‘opt-out’ of being identified.
4. Procedures for the use of tracking systems must be in accordance with these requirements as well as the requirements of the *Information Privacy Act 2014*, the *Human Rights Act 2004*, and the *Public Sector Management Act 1994* (the PSM Act).
5. Electronic controlled access systems are used to control access and entry to ACT Government buildings and assets. Such systems may include the recording of entry and exit from premises, rooms, lifts and doors. Records and logs of access and entry may be retained for specified periods. Wireless Access Point (WAP) logs could be used to determine someone's rough location within an ACT Government workplace.
6. GPS devices are used to track the location of ACT Government vehicles and other assets. In the case of field workers, a GPS device may be used to track the location of an individual worker or contractor.
7. Records of workplace surveillance are retained in accordance with the requirements of the *Territory Records Act 2002*. Where necessary or relevant surveillance records may be kept for a period longer than required under the *Territory Records Act 2002*.

### Who is regularly or ordinarily the subject of tracking surveillance?

1. Operators of ACT Government vehicles and mobile plant and equipment may be the subject of tracking surveillance.
2. Electronic controlled access systems (proximity cards, building access cards, entry swipe cards, etc) may also track access of ACT Government workers and contractors to ACT Government workplaces and other assets. Directorate workers engaged in field work may be subject to GPS devices.
3. Users of Cabcharge and Uber services will have their journey tracked; and location of users of desk booking systems will show intended booking locations.

### When tracking surveillance occurs

1. Tracking surveillance is ongoing. Where tracking surveillance is operating in an ACT Government vehicle or other thing, the tracking will operate when the vehicle or other thing is operating outside of the Territory.

# Purpose for Which Tracking Surveillance Records May be Used or Disclosed

### Security of ACT Government Workers and Assets

1. Tracking surveillance of workers and assets is in place to ensure the security and safety of ACT Government workers and assets, and for the safety and security of members of the public, and the security of ACT Government property and assets.

### Audit and Legal Requirements

1. Records of tracking surveillance may be audited, are subject to Territory and Federal laws, and may be used as evidence in legal proceedings, and administrative and/or disciplinary proceedings.

### Efficiency of ACT Government Business Activities

1. Tracking devices may be used for process control and business monitoring, such as to monitor the business utilisation of vehicles, equipment, assets, services and location.

## Misconduct and Underperformance

1. Directorates, public sector bodies, and the Public Sector Standards Commissioner, may rely on information captured by surveillance devices to investigate alleged breaches of ACT Government policies or the law, including section 9 of the PSM Act, by workers.
2. The Public Sector Standards Commissioner may at any time decide to instigate an investigation of alleged misconduct[[4]](#footnote-4).
3. Any such investigation and preliminary assessments will be carried out in accordance with the requirements of relevant enterprise agreements and the PSM Act, and in accordance with the principles of natural justice and procedural fairness.
4. Furthermore, tracking surveillance may be used in cases of suspected underperformance; in line with governing polices and Enterprise Agreements.

## Covert Surveillance

1. Any surveillance of a worker in a workplace outside the parameters of this Policy and notice is covert surveillance and must be authorised by a Magistrate in accordance with section 26 of the WP Act.

## Prohibited Surveillance

1. Section 41 of the WP Act prohibits:
2. surveillance not in accordance with an employer’s policy and notice to workers;
3. surveillance in a toilet facility, a change room, a shower or other bathing facility, a parent or nursing room, a prayer room, a sick bay, a first-aid room, and any other area in a workplace prescribed by regulation. Note: this does not prohibit data tracking surveillance and use of data to monitor the efficiency of government activities through the use of access proximity cards which may be used to open entrances to these facilities;
4. surveillance when the worker is not in a workplace, except in cases of data (computer) surveillance where the worker is using equipment, applications and/or resources supplied by the ACT Government and surveillance is restricted to the use of such equipment/services only;
5. any action that blocks emails unless a notice (a blocked delivery notice) has been given to the worker or where the incoming communication is perceived to be spam or a threat to the security of the Government or its information systems, or the email contains material that might reasonably be considered to be threatening, harassing or offensive; and
6. any action to prevent delivery of an email or access to a website because it has been sent by or on behalf of an industrial association or contains information about industrial matters.
7. The *Listening Devices Act 1992* provides that a person must not use a listening device with the intention of—
8. listening to or recording a private conversation to which the person is not a party; or
9. recording a private conversation to which the person is a party.

## Further Information

1. Please contact eba@act.gov.au if you would like further advice on the requirements or the application of this Policy.
1. Division 7.2 of the PSM Act provides a definition of eligible employment and a mechanism for working out certain entitlements for public servants. The Legislation Act defines ‘public servant’ as a person employed in the public service. Section 12 of the PSM Act establishes the ACT Public Service. It provides that members of the ACT Public Service are ‘the senior executive service’, ‘officers’ and ‘employees’. A senior executive service member is a person engaged under section 31 of the PSM Act. An officer is a person appointed to an office on a permanent basis (see section 24 PSM Act). An employee is a person employed to exercise the functions of an office on a temporary basis (see section 25 and part 5.8 PSM Act), which includes a person employed on a fixed term temporary or casual employment contract. The entitlement applies to ‘public sector members’ by virtue of section 150 of the PSM Act. A public sector member includes a statutory officeholder and a person employed by a statutory officeholder. [↑](#footnote-ref-1)
2. Certain provisions of the 2006 PSM Standards [DI2006-187] continue to apply, in accordance with part 10 of the 2016 PSM Standards. [↑](#footnote-ref-2)
3. *Workplace Privacy Act 2011* [↑](#footnote-ref-3)
4. Section G5.7 of the Enterprise Agreements, or however described. [↑](#footnote-ref-4)