Government of South Australia
Department of Human Services

Workplace Surveillance Devices Policy

Department of Human Services (DHS)

Summary

This policy governs how the Department for Human Services (DHS) manages use of all surveillance devices and recorded information, and complies with all relevant legislation.

Table 1: Document Details

Policy Number	FBS 051
Applies to	All DHS Staff and non-DHS staff
Issued by	Infrastructure, Finance & Business Services
Delegated Authority	Nick Ashley, Chief Financial Officer, Finance & Business Services
Policy Custodian	Suzanne McKell, Director, Infrastructure & Agency Securty Executive
Content author (position & phone no)	Carol Douglas, Manager Asset Services, Agency Security Advisor.
Implementation Date	November 2015
Approval Date	November 2017
Review Date	November 2022
Confidentiality	Public

Table 2 – Revision Record

Date	Version	Revision description
September 2017	2.0	Change to clause 5.1 in line with changes to AYTC Orders and updated to new template
October 2020	3.0	

Table of Contents

1. Policy Title

Workplace Surveillance Devices Policy

2. Purpose

The purpose of this DHS Workplace Surveillance Devices Policy is to:

- Provide information and direction on the use of surveillance devices in and associated with DHS workplaces and property, including the use of optical surveillance, listening or tracking devices; recording of private conversations; the use of information technology systems; and the communication and storage of data recorded / collected through surveillance.

- Facilitate compliance within DHS with:

    - The requirements of legislation, including the Surveillance Devices Act 2016 (SA); and

    - The Information Privacy Principals (IPPS) Instruction – Circular No. 12 issued by the Department of the Premier and Cabinet

as these apply to workplace surveillance in and by DHS.

3. Context

DHS is committed to providing safe, healthy and secure environments for all workers, clients and/or residents, contractors, students, volunteers, visitors and the public. Surveillance devices can assist in the promotion of safety, wellbeing, appropriate behaviours and improve security.

Department of Premier and Cabinet (DPC) circular PC012 – Information Privacy Principles Instruction regulates how South Australian Government agencies can collect, use, disclose, secure, provide access to and collect personal information. The use of listening and optical surveillance devices is also regulated by the Surveillance Devices Act 2016 and the Surveillance Devices Regulations 2017.

The Office of the Australian Information Commissioner (OAIC) can take regulatory and enforcement action to encourage and ensure compliance with privacy obligations. The OAIC's Privacy Regulatory Action Policy explains the OAIC's approach to using these privacy regulatory action powers.

4. Scope

This policy applies to:

- All DHS sites, workers, clients and/or residents, contractors, students, volunteers, visitors and the public

- All images and audio captured, recorded and/or stored for the purposes of security related monitoring, incident deterrent and response, investigations, police matters or legal proceedings.

This policy does not apply to:

Images and audio captured, recorded and/or stored for purposes not related to security such as DHS training, marketing, social media or printed material. These areas are addressed in related DHS policies including:

- Communication
- Social Media
- Creation, Caption and Control of Records Disposal
- Storage and Retrieval of Records
- Records Security
- Online Information and Services

5. Policy Detail

5.1 Compliance with the Surveillance Devices Act 2016

The Attorney-General's Department website "What you should know about the Surveillance Devices Act 2016" provides a concise summary of the provisions of the Surveillance Devices Act. Implications for surveillance in DHS workplaces are outlined below:

5.1.1 Consent from the surveillance subject required

Unless exceptions provided for by the SD Act apply, surveillance in and by DHS may only occur with the consent of the surveillance subjects. Consent to surveillance may be explicit (verbal or written agreement) or implied (where the persons under surveillance have been made aware of the surveillance). This awareness can be created by:

- Signage placed in prominent locations where surveillance devices are or may be used, including at the entrance to and around DHS sites;
- DHS polices, including this Policy, applicable to all employees, or
- The terms and conditions of the contracts, authorisations and licencing agreements to work on DHS sites of non-DHS workers such as contractors, students and volunteers.

5.1.2 Installation, use and maintenance of surveillance devices

With authorisation from the appropriate delegate (refer 5.3), surveillance devices as specified below may be installed, used and maintained in any workplace or property DHS deems appropriate in order to enhance safety, promote

appropriate behaviour, improve security, and record incidents. These areas will typically be entrances, reception areas, foyers, interview rooms, common areas, vehicles and car parks.

- A listening device that is used to listen to or record private conversations or words spoken to or by any person in private conversation without consent of all parties;

- An optical device that is used to observe or record visually (whether for still or moving pictures) a person, place or private activity without consent of all parties;

- A tracking device that is used to determine the geographical location of a person, vehicle or thing without consent. This does not prevent a person from using tracking technology to locate and retrieve an object such as a phone or computer; and

- A data surveillance device that is used to access, track, monitor or record the input or output of information from a computer without the person's consent.

Where surveillance devices are required to be installed in workplaces or property not owned by DHS, consent must be obtained by the lawful owner of the property.

5.1.3 Use of information, material or data from surveillance devices

Without authorisation from the appropriate delegate, or exempted by provisions under the SD Act, workers must not use, communicate or publish information or material derived from the use of a listening device or optical surveillance device in or around a DHS workplace.

5.2 Compliance with PC012 - Information Privacy Principles

PC012 - Information Privacy Principles (IPPs) apply to all public sector agencies. The IPPs are relevant to the use of surveillance devices across DHS because the information collected by these devices is typically private personal information. The key requirements of Part II of the IPPs are are outlined below as these relate to personal information derived from the use of surveillance devices across DHS.

5.2.1 Collection of Personal Information

IPP 1 requires that personal information should not be collected by unlawful or unfair means, nor should it be collected unnecessarily. Public sector agencies may only collect information through surveillance devices in their workplaces for legitimate reasons and relevant to its pupose and functions. Information collected by the use of surveillance devices must be acquired in a manner that adheres to legislative requirements and ethical standards where the right to privacy if individuals may be impacted.

5.2.2 Notice of Surveillance must be given

IPP 2 requires that, before personal information is collected by the use of surveillance devices, reasonable steps must be taken to advise individuals of:

- The purpose for collecting the information;
- Any authorisation of or legal requirements for collecing the information; and
- The use and disclosure of the information / material / data collected.

5.2.3 Irrelevant or excessively personal information must not be collected

IPP 3 requires that an agency should not collect personal information that is:

- Inaccurate, irrelevant, out of date, incomplete or excessively personal.

DHS must not collect information via surveillance which is not relevant to a legitmate purpose. All surveillance information collected by DHS must be:

- Directy related to the employment relationship between DHS and the worker;
- Directy related to non-DHS workers' contracts, authorisations and licensing agreements allowing non-DHS workers to work on or attend DHS sites;
- Related to the safety and security of its workers, clients and/or residents, contractors, students, volunteers, visitors and the public;
- Related to the protection of assets, information, integrity, reputation and other legitimate interests of DHS;
- Related to the prevention or investigation of alleged / suspected criminal activity or misconduct; or
- Other legitimate reasons (e.g. authorised or required by law).

Surveillance devices should not be used where there is a reasonable expectation of privacy, such as examination rooms, change rooms, bathrooms or toilets. Surveillance of this type could also be in contravention of section 26B or 26D of the *Summary Offences Act 1953* as it could lead to humiliating / degrading filming or indecent filming.

Safety and security requirements at the Kurlana Tapa Training Centre (KTTC) means that various surveillance devices will be used across all areas of the campuses. Use is defined and strictly managed in accordance with the applicable KTTC Orders. Where devices are placed in private areas; security staff must ensure cameras are positioned to protect dignity and privacy.

5.2.4 Storage of personal information

IPP 4 requires that public sector agencies must take such steps as are, in the circumstances, reasonable to ensure that personal information in its possession or under its control is securely stored and is not misused.

5.2.5 Access to records / recordings of personal information

IPP 5 requires that where an agency has in its possession or under its control records of personal information, access to those records may be obtained in accordance with the *Freedom of Information Act 1991.*

5.2.6 Use of personal information

IPPs 7 and 8 require that personal information collected via surveillance devices, should not be used by an agency for a purpose that is not the purpose of collection or a purpose incidental to or connected with that purpose (a secondary purpose) unless:

- the record-subject would reasonably expect the agency to use the information for the secondary purpose and the secondary purpose is related to the primary purpose of collection;
- the record-subject has expressly or impliedly consented to the use;
- the agency using the information believes on reasonable grounds that the use is necessary to prevent or lessen a serious threat to the life, health or safety of the record-subject or of some other person;
- the use is required by or under law;
- the use for that other purpose is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty or for the protection of the public revenue or for the protection of the interests of the government, statutory authority or statutory office-holder as an employer;
- the agency has reason to suspect that unlawful activity has been, is being or may be engaged in, and discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or
- the agency reasonably believes that the use relates to information about an individual that suggests that the individual has engaged or may engage in illegal conduct or serious misconduct in relation to a person; and
    - the agency reasonably believes that the use is appropriate in the circumstances; and
    - the use complies with any guidelines issued by the Minister for the purposes of this clause.

5.2.7 Disclosure of personal information

IPP 10 states that an agency should not disclose personal information about some other person to a third person for a purpose that is not the purpose of collection (a secondary purpose) unless:

- the record-subject would reasonably expect the agency to disclose the information for the secondary purpose and the secondary purpose is related to the primary purpose of collection;

- the record-subject has expressly or impliedly consented to the disclosure;
- the person disclosing the information believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious threat to the life, health or safety of the record-subject or of some other person;
- the disclosure is required or authorised by or under law;
- the disclosure is reasonably necessary for the enforcement of the criminal law, or of a law imposing a pecuniary penalty or for the protection of the public revenue or for the protection of the interests of the government, statutory authority or statutory office-holder as an employer;
- the agency has reason to suspect that unlawful activity has been, is being or may be engaged in, and discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or
- the agency reasonably believes that the disclosure relates to information about an individual that suggests that the individual has engaged or may engage in illegal conduct or serious misconduct in relation to a person; and
    - the agency reasonably believes that the disclosure is appropriate in the circumstances; and
    - the disclosure complies with any guidelines issued by the Minister for the purposes of this clause.

5.2.8 Unlawful activity, illegal or serious misconduct

A reasonable suspicison of unlawful activity, illegal or serious misconduct must be present for DHS to use personal information obtained via surveillance devices for a secondary purpose.

Collection and use of information collected via the use of surveillance devices for this purpose should be recommended by the DHS Protective Security Insider Threat Risk Assessment Group.

5.3 Use of Surveillance Devices in DHS

5.3.1 Approval for installation, use and maintenance of surveillance devices

Approval to install, use and maintain surveillance devices within DHS workplaces and property can be provided by one of the following delgates:

- Chief Executive (CE)
- Executive Director (ED) of the Division requesting surveillance
- Agency Security Executive (ASE)
- Agency Security Advisor (ASA)

- Information Technology Security Advisor (ITSA).

Any application to install, use or maintain surveillance devices should be designed, implemented and operated in full consultation with the ASA / ASE. Approval to install, use or maintain surveillance devices within DHS must be for legitimate reasons (refer 5.2.3) and must comply with legislation, the IPPs and this Policy.

5.3.2 Provision of notice for use of surveillance devices

Notice of surveillance in DHS workplaces or property must be provided prior to the commencement of surveillance, unless:

- the surveillance is subject to a specific exemption by the CE (refer 5.3.#); or
- the surveillance is by and/or authorised by a person in a law enforcement agency or an inquiry agency as defined in the *Independent Commissioner Against Corruption Act 2012*.

Notice of use of surveillance devices is required as follows:

- Signage must be erected at the entrance to areas under optical surveillance to advise employees and others that they are entering an area under such surveillance. Signage should address language barriers, including the use of symbols.
- Workers must be advised of the provisions of this Policy (e.g. in hard copy) and must be able to access this Policy on the DHS intranet and internet.
- New workers must be advised of their obligations to comply with DHS policies, when commencing work (e.g. during induction).
- Non-DHS workers, students and volunteers must be made aware of the requirements of this Policy through the terms and conditions of their contracts or agreements authorising them to work on or attend DHS sites.
- As necessary, all workers should periodically be reminded of (the possibility of) surveillance in DHS facilities and by authorised employees of DHS.
- Where new surveillance in a specific area is intended, workers and relevant worker associations have to be provided 14 days' advance notice of:
    - the kind of surveillance intended (e.g. camera, computer, or tracking);
    - the reasons for the surveillance;
    - authorisation of, or legal requirements of the surveillance;
    - when the surveillance will commence / conclude;
    - whether the surveillance will be continued or intermittent;
    - whether surveillance will be for a specified limited period or ongoing; and

- the use and disclosure of the information collected.

5.3.3 Use of optical surveillance devices

Optical surveillance devices (video cameras) must be installed in a clearly visible manner in the location where the surveillance is to occur (i.e. must not be covert).

As per 5.3.1, any request for new optical surveillance must be approved by one of the delegates specified. It is recommended that advice from the ASE / ASA is sought in relation to such approvals and address criteria as per 5.3.2.

5.3.4 Prohibited use of optical surveillance devices

Surveillance devices should not be used where there is a reasonable expectation of privacy, such as examination rooms, change rooms, bathrooms or toilets.

Safety and security requirements at the Kurlana Tapa Training Centre (KTTC) means that various surveillance devices will be used across all areas of the campuses. Use is defined and strictly managed in accordance with the applicable KTTC Orders. Where devices are placed in private areas; security staff must ensure cameras are positioned to protect dignity and privacy.

5.3.5 Use of listening surveillance devices

The installation,use and maintenance of listening devices to overhear, record, monitor or listen to private conversations is prohibited. Unless exemptions under sections 4 and 6 apply, private conversations must not be recorded and optical surveillance, whether overt or covert must not contan listening devices or have the ability to record private conversations.

Exemption to sections 4 and 6 apply where:

- The parties to the conversation consent to use of a listening device.
- A listening device is needed to protect the lawful interests of a person.
- The use of the device is in the public interest.
- The use is specifically authorised by legislation (e.g. the *Telecommunications (Interceptions) Act 1979* (Cth); *Part 2 of the Criminal Investigation (Covert Operations) Act 2009;* or the *Security and Investigation Industry Act (1995*).

5.3.6 Use of covert surveillance devices

Covert surveillance must not be used except for the purposes of detecting suspected unlawful / criminal activity in the workplace. It may not be used to monitor employees (e.g. whether they are present, performing as required or for any other monitoring purpose).

Should a site need to install listening and optical surveillance devices for the purpose of covert surveillance as part of an investigation, the Office of the CE

should be contacted, and this can only be done in conjunction with an investigating agency under Part 2 - sections 4 and 5 and Part 3 of the Surveillance Devices Act SA 2016.

Investigating agencies are defined in the Act as:

- South Australian Police (SAPOL);
- Independent Commissioner Against Corruption (ICAC);
- the Australian Crime Commission (ACC);
- An enforcement agency within the meaning of the Telecommunications (Interception and Access) Act 1979 of the Commonwealth; or
- A police force of a participating jurisdiction.

Where the use of covert surveillance has been recommended, a formal written request must be made to the CE addressing criteria in 5.3.2 and the following:

- the basis of the suspicion that one or more employees are involved in unlawful activity;
- any agency/ies that the suspected conduct has been reported to (e.g. the Office for Public Integrity; the Independent Commission Against Corruption or the SA Police – Anti-Corruption. Branch); and
- whether any other managerial or investigative procedures have been undertaken to detect the unlawful / criminal activity and the outcome of these procedures.

The apparent seriousness of the suspected unlawful activity will determine whether there are sufficient grounds for covert surveillance.

The CE must be satisfied that the covert surveillance of the worker (s) will not unduly intrude on the privacy of any other individual; and should be able to justify their approval of the covert surveillance should the Privacy Committee of South Australia investigate complaints relating to the covert surveillance or regarding alleged violations of individual privacy.

5.3.7 Surveillance of use information and communications technology (ICT)

DHS has a responsibility to protect and monitor the content of information sent through its electronic communications. Such monitoring is undertaken for all DHS electronic communications activities.

DHS workers' and non-DHS workers's use of ICT (e.g. emails, use of the internet or access to databases) may be monitored for legitimate purposes; e.g. to ascertain that the use of ICT systems, computers, databases and related facilities is appropriate; to investigate suspected or alleged breaches of acceptable use; or as part of an investigation of suspected/alleged misconduct or illegal activity.

Under certain circumstances, the Chief Executive, ELT or the ASE/ITSA may approve requests to report on or investigate email and internet activities. This may involve accessing, reviewing and disclosing details of electronic communications use. (Refer to DHS Information Security Policy).

5.3.8 Monitoring of access to DHS workplaces

The Chief Executive, EDs or those with delegated authority (minimum HR delegation Level 4) may, for purposes stated under 5.2.3, approve monitoring of individual worker's access to DHS workplaces or property (e.g. via examining the use of security access cards or by existing optical surveillance).

5.3.9 Tracking of DHS vehicles

The Chief Executive, EDs or those with delegated authority (minimum HR delegation Level 4) may, for purposes stated under 5.2.3, approve the use of tracking devices indicating the geographical location of DHS vehicles. It is recommended that advice form the ASE / ASA is sought for such approvals.

5.3.10 Investigative Surveillance

The Chief Executive, EDs or those with delegated authority (minimum HR delegation Level 4) may approve the use of investigative surveillance (refer 5.3.2 and 5.3.6). The investigating officer must provide the CE, ED or ITSA a brief synopsis of the following:

- The allegations/complaint being investigated.
- The nature of surveillance required.
- The purpose of the surveillance and how the data obtained will be used.
- How the information obtained will be safeguarded and managed.
- The individuals/authorities that will be involved in the investigation and will have access to the data obtained.
- Duration of the surveillance or indication of when the investigative investigation will be concluded (e.g. reference to date or an event.)

5.3.11 Surveillance related to workers compensation

Pursuant to the IPPs, DHS, must at all times respect an injured employee's integrity, confidentiality of their personal information and right to privacy. A reasonable suspicion of dishonesty or fraudulent activity must therefore be present before surveillance of an injured worker may commence. This surveillance must therefore only be approved in such circumstances. The Executive Director People, Strategy and Systems, Director Incident Management Unit or Director Human Resources, Wellbeing and Safety may approve this.

5.4 Access to Data

In DHS, access to data / information derived from surveillance is restricted to the CE, EDs, ASE, ASE, ITSA or those with delegated authority (minimum HR delegation Level 4).

Only workers approved by the ASE, ASA, ITSA, Executive Director Disability Services, Executive Director People, Strategy and Systems, Executive Director Youth Justice, or a worker directed by the Chief Executive (CE) may access recorded material to review incidents. Recorded material may also be used in relation to:

• The detection, investigation or prosecution of any unlawful activity

• Determining the sequence of events and actions during an incident

• Supporting workers when reporting incidents or facing complaints or allegations.

Retrieval of data / information should be approved by the executive responsible for the business unit or site. If the matter relates to a worker, consultation with a senior manager or executive in the People, Strategy and Systems Division is required (and evidence supplied) before approval to retrieve data / information is granted.

Data from optical devices should be retrieved by an authorised security technician and supplied only to the person authorised and requesting the information. The technician may also deliver the information to an authorised law enforcement or inquiry agency directly.

Part 3, Divisions 1-3 of the Surveillance Devices Act govern the procedure for an investigation agency to make an application for a warrant. Part 3, Divisions 5 and 6 of the SD Act govern the investigation agency's obligations to maintain control of records and govern the agency's reporting requirements in relation to the same. Sections 32 and 33 of the SD Act legislate the powers of a review agency to ensure the investigating agency complies with its obligations.

Provision of information to a law enforcement or investigation agency is by the approval of the ASE, ASA, ITSA, Executive Director Youth Justice, Executive Director Disability Services, Executive Director People, Strategy and Systems or the CE.

If DHS is required to provide information to a law enforcement or investigation agency, in most circumstances a worker, volunteer etc. identified in the footage will be notified, especially if the footage is for use in court and/or to be released to the media.

Other than when providing information to a law enforcement or inquiry agency as required, a delegate must not give others access to information/material derived from surveillance, unless the disclosure is:

- for a legitimate purpose related to the employment of staff or other legitimate business activities of DHS;
- for the purpose of responding to an application under the *Freedom of Information Act 1991;*

- for a purpose that is directly or indirectly related to civil or criminal proceedings (where authorised); or

- of such a nature that they reasonably believe it to be necessary to avert an imminent threat of serious violence or of substantial damage to property.

DHS may be required to provide information to a court pursuant to a court order such as summons or subpoena. In the event that a summons or subpoena is received, please contact the office of the Chief Executive who may refer to the matter to the Crown Solicitors Office (CSO).

After completion of any investigation or incident, the CE, ASE or the Executive Director Youth Justice may approve the release of the information / material for internal review and training purposes if appropriate.

Any delegate or decision maker with an actual or perceived conflict of interest in specific surveillance data must not access such information and must withdraw from decision-making on the matter.

Surveillance information must not be accessed:

- in ways which are inconsistent with the obligation on decision makers to act impartially;

- to improperly cause harm, detriment or embarrassment to any person or body;

- to improperly influence others in the performance of their duties or functions;

- for voyeuristic purposes;

- for the advantage of any person or body; or

- to justify the acceptance of any immediate or future gift, reward or benefit from any person or body for themselves or for any other person or body.

Any worker acting contrary to these requirements, i.e. inappropriately accessing personal information, may be liable to disciplinary action.

5.5 Retention, download and Storage of surveillance data

All material derived from surveillance activities is deemed the property of the state under the *State Records Act 1997* and DHS is responsible for the security and proper preservation of these records. The Department is required to register, store and retain records according to the agreed *Disposal Schedules* issued under the Act.

DHS must take reasonable steps to ensure that personal information from surveillance in its possession or under its control is securely stored and is not misused - consistent with IPP 4. Records must be classified according to the "*Information Security Policy*".

Where data is required to be physically stored, it must be downloaded/copied onto an appropriate storage device, such as a compact disc, USB flash drive or hard drive and kept in secure storage. Approved persons must ensure that the

data is protected against loss, unauthorised access, disclosure, modifications and/or other misuse. Security measures may further include:

- physical measures, e.g. locks and swipe cards for monitoring data storage areas; or
- electronic measures, e.g. passwords for accessing the surveillance equipment; including access, retrieval, copy and encryption of the data.

All requests to retrieve data/information derived from surveillance activities must be submitted to DHS Security Services using the *DHS Request for CCTV Vision form*. Where data is downloaded/copied by an approved person, a register must be kept which details:

- the record of the approval to commence extraction and retention of this data;
- the date the data was downloaded or copied;
- the location of the camera;
- the date the data was captured by the camera;
- a brief description of the incident that has been downloaded/copied;
- the time period covered by the downloaded/copied footage;
- the purpose for which the data was downloaded/copied e.g. evidentiary purposes for suspected criminal activity and/or misconduct in the workplace or in response to an FOI request;
- the recipient of the data;
- the medium onto which the data was downloaded/copied;
- the title of the record and the location where the copied data will be stored;
- the name and signature of the authorised person who downloaded or copied the data; and
- The name and signature of the authorised person who received the the data.

Where data is downloaded/copied and provided to SAPOL for evidentiary or investigative purposes, a SAPOL field receipt must be obtained from the requesting Police and recorded in the above register.

The minimum storage capacity of DHS recording devices is as specified in the *State Records Act 1997* and the General Disposal Schedule for State Government. Compliance is reviewed regularly by the DHS Protective Security Committee.

Storage time limits for records relating to critical incidents and to assist with investigations are determined by the ASE, ASA, ITSA or Executive Director People, Strategy and Systems in consultation with the Manager, Business Services and/or as directed by the Chief Executive (records authorities). Records of reported and critical incidents will be retained in accordance with the relevant

General Disposal Schedule or the Operational records disposal schedule. The records authority may authorise the destruction of a record in accordance with the *Disposal, Storage and Retrieval of Records Policy* and the *Destroying Official Records flowchart*.

5.6 Surveillance in Disability or Aged Care workplaces

For quality, safety and security reasons, DHS may install or facilitate reasonable surveillance within and around its disability or aged care workplaces, including in common and public areas; and - after consultation with stakeholders - in private areas with the consent of the care recipients and/or others legally able to act on their behalf. Surveillance in common areas is conditional on clear signage notifying staff, care recipients and visitors of this surveillance.

It is recommended that written consent to surveillance is obtained from surveillance subjects in circumstances where there exists a reasonable expectation of privacy.

To facilitate installation and use of surveillance in private areas, Accommodation Services, (in consultation with stakeholders) may:

- Develop guidelines/procedures for the installation and use of this surveillance in bedrooms or private areas of disability care recipients (if requested or consented to by care recipients and/or by those with the legal authority to act on their behalf).

- Provide a standard consent agreement between DHS and a disability care recipient (and/or by those with the legal authority to act on their behalf) consistent with the above requirements.

The collection of audio or optical data must comply with the IPPs as per section 5.2 of this policy, in particular the use of personal information to be used for the purpose for which the data is being collected.

5.7 Surveillance in Kurlana Tapa Training Centre

Under the *Youth Justice Administration Act 2016*, the Minister mayu establish such training centres and other facilities and programs as the Minister thinks necessary or desirable for the care, rehabilitation, detention, training or treatment of youth.

It is the responsibiloity of the CE to ensure adequate arrangejents are in place at the training centre to, among other things:

- Maintain the physical, psychological and ernotional well being of the residents of the centre;

- Maintain discipline and order among the residents of the centre;

- Ensure, through implementation of operational procedures, the proper security, control and management of the centre;

- Keep proper records relating to the operation and management of the centre; and

- Ensure the good management of the centre.

The use of surveillance devices to monitor both residents and staff within the training centre environment could be considered consistent with the responsibilities of the CE in ensuring the proper security, control and management of the centre.

The collection of audio or optical data must comply with the IPPs as per section 5.2 of this policy, in particular the use of personal information to be used for the purpose for which the data is being collected.

The primary purpose for using surveillance devices in the training cnetre environment is broad and encompasses *ensuring the safety and protection of staff, residents and visitors and contributing to security*.

Whilst the footage may have been gathered for one purpose, the IPPs do not preclude using the footage for staff compliance with operational requirements in this setting. Use of footage on this manner, supports the CE in enuring adequate arrangements are in place at the training centre.

With regards to IPP 2 which states that reasonable steps must be taken to provide notice of the use of surveillance devices, staff at the training centre are permitted to have cameras activated at all times for security purposes wiothout verbally notifying residents or nearby personnel. Residents must be advised upon their entry to the centre, that surveillance devices are in use and desctibe how the data is recorded and maintained.

If data needs to be recorded outside of the centre; ie at court, hospital, funeral, etc, the definition of private place vs public place needs to be considered. It is likely that the areas (as above) being recorded outside of the centre will satisfy the definition of a public place and footage captured by surveillance devices is permitted.

If staff entered a private property, they would need to seek permission from other people gathered to record footage. If the footage in a private setting is required for the safety of the staff member, then section 5.4.b of the SD Act which exempts the use of a surveillance device if *reasonably necessary for the protection of the lawful interests of that person* will apply.

5.6 Procedures

DHS business units should develop a local procedure in accordance with this policy appropriate for the type of service and site, and consistent with statutory responsibilities and legal obligations.

A local procedure needs to consider the nature of the business and management structure of a site. Where a site or building comprises several business units, the manager with overall responsibility for the site or campus is responsible for developing a local procedure. DHS Security Services may be contacted to review and provide comment on a draft procedure and to assist when surveillance devices are managed and operated by a third party outside DHS.

Include all the principles, rules, assumptions and responsibilities associated with the implementation and achievement of the policy. Provide sufficient detail so

workers are clear about what they must do, in order to be compliant with the policy.

6. Risk

Ineffective management and access to recorded information derived from surveillance activies owing to a lack of a departmental policy may result in breaches in the Department's legislative requirements and expose DHS to legal action.

7. Definitions

Listening Device means-

- A device capable of being used to listen or to record a private conversation or words spoken to or by any person in prvate conversation (whether or not the device is also capable of operating as some kind of surveillance device); and
- Associated equipmentr (if any).

Optical Surveillance Device means-

- A device capable of being used to observe ro record visually (whether for still or moving pictures) a person, place or activity; and
- Associated equipment (if any).

Tracking Device means-

- A device capable of being used to determine the geographical location of a person, vehicle or thing; and
- Associated equipment (if any).

Data Surveillance Device means-

- A program or device capable of being used to access, track, monitor or record the input of information into, or the output of information from, a computer; and
- Associated equipment (if any)

Surveillance Device means-

- A listening device; or
- And optical surveillance device; or
- A tracking device; or
- A data surveillance device; or

- A device that is a combination of any of the deivces referred to in a preceeding paragraph; or

- A device of a class or kind prescribed by the regulations.

Aged care means aged care facilities managed by DHS; including residential aged care facilities (Commonwealth funded) and accommodation options for older people (state funded).

consent means that an individual has authorised their personal information to be used for a defined purpose or handled in a particular manner. Consent may be expressed (i.e. given orally or in writing) or implied (i.e. reasonably inferred from the conduct of the individual).

Disability Care means facilities managed by DHS; including small residential facilities providing accommodation options for people with disabilities.

Primary purpose means the dominant purpose for which information is collected. Most often in the health system the primary purpose will be to provide care, or an episode of care.

Private Activity means:

- An activity carried on by only 1 person in circumstances that may reasonably be taken to indicate that the person does not desire it not to be observed by any other person, but does not include:
    - An ctivity carried on in a public place; or
    - An activity carried on or in premises or a vehicle if the activity can be readily observed from a public place; or
    - An activity carried on in any other circumstances in which the person ought reasonably to expect that it may be observed by some other person; or
- An activity carried on by more than 1 person in circumstances that may reasonably be taken to indicate that at least 1 party to the activity desires it to be observed only by the other parties to the activity, but does not include:
    - An activity carried on in a public place; or
    - An activity carried on or in premises or a vehicle if the activity can be readily observed from a public place; or
    - An activity carried on in any otjher circumstances in which a party to the activity ought reasonably to expect that iot may be observed by a person who is not a party to the activity.

Public Place includes:

- A place to which free access is permitted to the public, with the express or tacit consent of the owner or occupier of that place; and
- A place to which the public are admitted on payment of money, the test of admittance being the payment of money only; and
- A road, street, footway, court, alley or thoroughfare which the public are allowed to use, even though that road, street, footway, court, alley or thoroughfare is on private property.

Reasonable suspicion means there is a rational basis for the suspicion, i.e. the suspicion is based on facts and those facts are plausible.

Secondary purpose means the use or disclosure of personal information for a purpose other than the purpose for which it was collected.

Worker is a person that carries out work in any capacity for DHS on DHS sites including employees, contractors, sub-contractors, trainees, work-experience students or volunteers or contractors employed by and/or representing or attending DHS sites (including any of its divisions or offices) or representing DHS in an official capacity.

8. Reference Documents

8.1 Directive documents

- Adelaide Youth Training Centre Orders
- Australian Standard AS4806.1 – 2006 Closed Circuit Television – Management and Operation
- Code of Ethics for the SA Public Sector
- Criminal Law Consolidation Act 1953 (SA)
- Dirctions and Guidelines of the Independent Commissioner Against Corruption
- DPC Circular PC012 – Information Privacy Principles Instruction 2017
- Guardianship and Administration Act 1993
- Mental Health Act 2009
- Public Sector Act 2009 (SA)
- Residential Tenancies Act 1995
- State Records Act SA 1997
- Surveillance Devices Act 2016

- Surveillance Devices Regulations 2017
- Work Health and Safety Act 2012
- Youth Justice Administration Act 2016

8.2 Supporting documents

- CCTV Booklet 2018 (SAPOL)

8.3 Related documents and resources

- Office of the Australian Information Commissioner http://www.oaic.gov.au
- Information Classification and Handling Policy
- General Disposal Schedule No. 30 for the retention of CCTV records
- Disposal, Storage and Retrieval of Records Policy

9. Aboriginal Impact Statement Declaration

The needs and interests of Aboriginal people have been considered in the development of this policy and there is no direct impact on Aboriginal people.

Policy Approval

Content Author: Carol Douglas Agency Security Advisor Manager, Asset Services Phone: 70414 Date: / /	…… Suzanne McKell Agency Security Executive Director, Infrastructure, Finance & Business Services / /	..... Nick Ashley A/Executive Director, Finance & Business Services / /
Comments:	**APPROVED / NOTED** ---------- **Lois Boswell** **Chief Executive** / /	