DISTRICT COUNCIL OF Streaky Bay
29 Alfred Terrace, Streaky Bay SA 5680
T: (08) 8626 1001 **E:** dcstreaky@streakybay.sa.gov.au

SURVEILLANCE POLICY

Policy No: **DCSB-IFM-13.04**	Approved on: **18 March 2025**	Administered by: **Chief Executive Officer**
Last Reviewed: **March 2025**	Review Date **March 2027**	Record No: **448998**
Classification: **Health & Safety**		

Strategic Plan link:
Strategy 1.1.7 Ensure compliance of relevant Council policies and procedures with legislative requirements.

References and related Policies, Procedures and Forms:
Development Act 1993
Dog and Cat Management Act 1995
Freedom of Information Act 1991
Local Government Act 1999
Local Nuisance and Litter Control Act 2016
Planning, Development, and Infrastructure Act 2016
Road Traffic Act 1961 – Australian Road Rules
State Records Act 1997
Summary Offences Act 1953
Surveillance Devices Act 2016 (SA)
Work Health and Safety Act 2012
Australian Standard 4806.1 – Closed Circuit Television (CCTV) Management and Operation – Code of Practice
Australian Standard 4806.2 – Closed Circuit Television (CCTV) Application Guidelines
Information Standards IS40 – Recordkeeping
Information Standards IS40 – Retention and Disposal of Public records

Contents

1. Definitions 5
2. Introduction 5
3. Purpose 5
4. Scope 6
5. Surveillance devices 6
6. Policy 7
7. Justification for use of CCTV 7
8. Locations of Cameras 8
9. Covert Surveillance 8
10. Notification and Signage 8
11. Retention of Data 8
12. Access 8
13. Police Requests 9
14. Access Requests 9
15. Responsibilities 9
16. Review 10
17. History 10

1. Definitions

Closed-Circuit Television (CCTV)	is a system used for audio and visual video surveillance using video cameras and microphones and transmitting the recorded data to a recording device or monitor(s).
Council	refers to the Local Government Authority of the District Council of Streaky Bay
Data (processing, processor, controller, subject)	information in a form that can be processed. It includes automated or electronic data - any information on computer or information recorded with the intention of putting it on computer; and manual data - information that is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system.
Personal Data	relates to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller.
Mobile Optical Surveillance Devices and Listening Devices	means a mobile device capable of being used to observe or record (whether for still or moving pictures) a person, place, or activity. Includes devices, such as body cameras
Fixed Optical Surveillance Devices	means a fixed device capable of being used to observe or record visually (whether for still or moving pictures) a person, place, or activity. Includes devices, such as CCTV
Audio/Visual Recording	means any recording captured on Fixed Optical Surveillance Device or a Mobile Optical Surveillance Devices and Listening Devices.
Tracking devices	Tracking devices can record the exact position of the targeted entity at specific time intervals. Includes devices, such as IVMS, Lone Workers Devices etc
Relevant Act	"Relevant Act" means the *Local Government Act 1999*, *Local Nuisance and Litter Control Act 2016*, *Development Act 1993*, *Planning, Development and Infrastructure Act 2016*, *Dog and Cat Management Act, Road Traffic Act 1961 – Australian Road Rules* and any other Act where Council has enforcement or regulatory functions, which for completeness does not include the *Surveillance Devices Act 2016 (SA)*.

2. Introduction

Surveillance systems are installed on the District Council of Streaky Bay (Council) assets including Council buildings and vehicles.

3. Purpose

3.1. Surveillance devices may be deployed within the workplace in order to protect the assets and equipment of Council and improve community and employee safety. Council is committed to:

3.1.1. Providing a safe environment for its employees and the community in which unlawful, antisocial, and inappropriate activity is kept to a minimum while respecting individual rights to privacy.

3.1.2. Complying with the requirements of the relevant legislation and associated directions including the Surveillance Devices Act 2016 (SA) and the Freedom of Information Act 1991

3.1.3. Explaining to employees, contractors, visitors, and volunteers (collectively referred to as employees in this policy) the circumstances when workplace surveillance will be undertaken.

4. Scope

4.1. The scope of this policy is to regulate the use of any workplace surveillance devices and associated technology in the monitoring of both the internal and external environments of public and workplace facilities and assets owned or managed by Council.

4.2. This policy relates directly to the location and use of the workplace surveillance and monitoring, recording and subsequent use of such recorded material.

4.3. This policy applies to the public and all employees engaged or appointed by Council of while on the Council's premises or while engaged in Council related activities.

4.4. This policy constitutes a lawful instruction to employees. Any breach of this policy may lead to disciplinary action including, but not limited to, termination of employment or engagement with Council.

5. Surveillance devices

5.1. Fixed Optical surveillance devices

5.1.1. Council may deploy fixed optical surveillance devices, including closed circuit TV cameras (CCTV) or video cameras, to monitor or record activities on Council premises. Surveillance devices may be installed by Council in areas where assets or equipment are stored or commonly used, outside Council buildings or in high-risk work areas.

5.1.2. Surveillance devices will be installed in a location where they are clearly visible, and the Council will erect signs to inform employees and community members that surveillance devices are in use. Surveillance devices will not be placed inside bathrooms, change rooms, residences, or in such a position as to view inside these premises.

5.2. Tracking devices

5.2.1. Global positioning systems (GPS) or tracking devices may be utilised in vehicles or equipment for the purpose of monitoring and recording geographical location or movement.

5.2.2. The District Council may install a GPS or tracking device where:

- the operator/driver of a vehicle or equipment is required to work alone
- there are safety or other risks associated with the tasks being carried out by an employee, or
- there is a need to monitor and protect specific assets or equipment.

5.2.3. Vehicles or equipment with GPS or tracking devices fitted will have a sticker stating that such a device has been fitted.

5.3. Mobile Optical Surveillance Devices and Listening Devices

5.3.1 Council officers may utilise Mobile Optical Surveillance Devices and Listening Devices to record vision and/or sound that relates to their powers under a Relevant Act, including to record evidence of an offence being committed under one of those Acts. For example, Council officers may use Mobile Optical Surveillance Devices and Listening Devices to record a dog wandering at large, or a conversation between a resident and a Council officer where a local nuisance is being enforced, subject to 5.3.2 and 5.3.3.

5.3.2 Council officers equipped with mobile Optical Surveillance Devices and Listening Devices must identify themselves and advise that a Mobile Surveillance Device and/or Listening Device is in use when interacting with members of the public.
Members of the public continuing to engage with the Council officer are taken to consent to be recorded.

5.3.3 Council officers equipped with a mobile Optical Surveillance Device and/or Listening Device must ensure that the equipment is clearly visible to members of the public. No Optical Surveillance Device or Listening Device may be concealed by a Council officer.

6. Policy

6.1. General Principles

6.1.1. The District Council of Streaky Bay as the corporate body has a statutory responsibility for the protection of its property, equipment and other plant as well providing a sense of security to its employees, and invitees to its premises. Council has a duty of care under the provisions of Safety, Health and Welfare at Work Act and associated legislation and utilises surveillance systems and their associated monitoring and recording equipment as an added mode of security and surveillance for the purpose of enhancing the quality of life of the Council and community by integrating the best practices governing the public and private surveillance of its premises.

6.1.2. The use of the CCTV system will be conducted in a professional, ethical and legal manner and any diversion of the use of CCTV security technologies for other purposes is prohibited by this policy e.g. CCTV will not be used for monitoring employee performance.

6.1.3. Information obtained through the CCTV system may only be released when authorised by the CEO. Any requests for CCTV recordings/images from the Police will be fully recorded and legal advice will be sought if any such request is made. (See “Access” below). If a law enforcement authority, is seeking a recording for a specific investigation, it may require a warrant and accordingly any such request made by Police should be requested in writing and the Council may seek legal advice.

6.1.4. CCTV monitoring of public areas for security purposes will be conducted in a manner consistent with all existing policies adopted by the Council.

6.1.5. This policy prohibits monitoring based on the characteristics and classifications contained in equality and other related legislation e.g. race, gender, sexual orientation, national origin, disability etc.

6.1.6. Video monitoring of public areas for security purposes within Council premises is limited to uses that do not violate the individual’s reasonable expectation to privacy.

6.1.7. Information obtained in violation of this policy may not be used in a disciplinary proceeding against a workplace participant or a customer attending any of Councils facilities.

6.1.8. All CCTV systems and associated equipment will be required to be compliant with this policy following its adoption by the Council.

7. Justification for use of CCTV

Data collected via CCTV must be adequate, relevant, and not excessive for the purpose for which it is collected. This means that Council needs to be able to justify the obtaining and use of personal data by means of a CCTV system. The use of CCTV to control the perimeter of the buildings for security purposes has been deemed to be justified by the Council. The system is intended to capture images of intruders or of individuals damaging property or removing goods without authorisation.

8. Locations of Cameras

The location of cameras is a key consideration. Use of CCTV to monitor areas where individuals would have a reasonable expectation of privacy would be difficult to justify. Council has endeavoured to select locations for the installation of CCTCV cameras which are least intrusive to protect the privacy of individuals. Cameras placed so as to record external areas are positioned in such a way as to prevent or minimise recording of passers-by or of another person's private property.

9. Covert Surveillance

District Council of Streaky Bay will not engage in covert surveillance, unless authorised by the CEO and being identified as being necessary to an investigation relating to powers under a Relevant Act, i.e., installation of a Temporary Mobile Optical Surveillance Device in a remote area where illegal dumping has been occurring as part of their investigation into the enforcement of provisions under the Local Nuisance and Litter Control Act 2016.

10. Notification and Signage

The CEO will provide a copy of this Surveillance Policy on request to staff, Councillors, and visitors. Notification will include a contact number for those wishing to discuss CCTV monitoring and location of CCTV cameras. Adequate signage will be placed at each location in which CCTV camera(s) is sited to indicate that CCTV is in operation and at the entrance to Council property. Appropriate locations for signage will include at entrances to premises i.e. external doors, workshop gates.

11. Retention of Data

11.1. Images and data recordings that indicate unauthorised or inappropriate activity, either through a record of that activity or due to interference with the surveillance device, are to be referred to the Chief Executive Officer (CEO) for investigation. The CEO will retain the images and/or data and any associated information in a secure and confidential location.

11.2. The images or data recordings captured by the surveillance system will be retained for a maximum of 28 days, except where the image identifies an issue and is retained specifically in the context of an investigation/prosecution of that issue.

11.3. The images/recordings will be stored in a secure environment with a log of access kept. Access will be restricted to authorised personnel. Supervising the access and maintenance of the surveillance System is the responsibility of the CEO. The CEO may delegate the administration or maintenance of the CCTV System to another staff member or an authorised contractor. In certain circumstances, the recordings may also be viewed by other individuals in order to achieve the objectives set out above (such individuals may include the Police). When surveillance recordings are being viewed, access will be limited to authorised individuals on a need-to-know basis.

11.4. Surveillance data will be stored in a secure environment with a log of access to tapes kept. Access will be restricted to authorised personnel. Similar measures will be employed when using disk storage, with automatic logs of access to the images created.

12. Access

12.1. Surveillance data records and the surveillance equipment will be securely stored in a restricted area. Unauthorised access to that area will not be permitted at any time. The area will be locked when not occupied by authorised personnel. A log of access to surveillance data records will be maintained.

12.2. Access to the surveillance equipment and surveillance data records will be restricted to authorised personnel only, and in relevant circumstances. Surveillance data records may only be accessed:

12.2.1. By Police where District Council of Streaky Bay are required by law to make a report regarding the commission of a suspected crime; or

12.2.2. Following a request by Police when a crime or suspected crime has taken place and/or when it is suspected that illegal/anti-social behaviour is taking place on Council property; or

12.2.3. To data subjects (or their legal representatives), pursuant to an access request where the time, date and location of the recordings is furnished to Council; or

12.2.4. To individuals (or their legal representatives) subject to a court order; or

12.2.5. To Council's insurance company where the insurance company requires

13. Police Requests

13.1. Information obtained through video monitoring will only be released when authorised by the CEO. If police request CCTV images for a specific investigation, Police may require a warrant and accordingly any such request made by Police should be made in writing and Council should immediately seek legal advice.

14. Access Requests

14.1. Access to Audio/Visual Recordings by members of the public (including the media) is facilitated by the Freedom of Information Act 1991 (FOI Act). The Freedom of Information (FOI) process applies to Audio/Visual Recordings as it does other records and documents held by Council.

14.2. Any application received under the FOI Act must be determined by an accredited Freedom of Information Officer. If the application is approved, a member of the public may then listen/view the recording at Council's Main Office or obtain a copy of the requested Audio/Visual Recording within a timeframe that is reasonable and appropriate. If viewing at the Council's Main Office, an accredited FOI Officer, or a staff member delegated by the Chief Executive Officer (CEO) will always be present to operate the equipment.

15. Responsibilities

The Council Chief Executive Officer is responsible to:

a) Ensure that the use of CCTV systems is implemented in accordance with the policy set down by Council.

b) Oversee and co-ordinate the use of CCTV monitoring for safety and security purposes within Council.

c) Ensure that all existing CCTV monitoring systems will be evaluated for compliance with this policy.

d) Ensure that the CCTV monitoring at Council is consistent with the highest standards and protections.

e) Review camera locations and be responsible for the release of any information or recorded CCTV materials stored in compliance with this policy.

f) Maintain a record of access (e.g. an access log) to or the release of tapes or any material recorded or stored in the system.

g) Ensure that monitoring recorded tapes are not duplicated for release.

h) Ensure that the perimeter of view from fixed location cameras conforms to this policy both internally and externally.

i) Will provide a list of the CCTV cameras locations and the associated monitoring equipment and the capabilities of such equipment to Council for formal approval.

j) Approve the location of temporary cameras to be used during an investigation of a relevant act and ensure their withdrawal following the conclusion of the investigation.

k) Give consideration to feedback/complaints regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment

l) Ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals and be mindful that no such infringement is likely to take place

m) Advise the Council that adequate signage at appropriate and prominent locations is displayed as detailed above.

n) Ensure that external cameras are non-intrusive in terms of their positions and views of neighbouring residential housing and comply with the principle of "Reasonable Expectation of Privacy".

o) Ensure that monitoring tapes are stored in a secure place with access by authorised personnel only.

p) Ensure that images recorded on tapes/DVDs/digital recordings are stored for a period not longer than 28 days and are then erased unless required as part of a criminal investigation or court proceedings (criminal or civil) or other bona fide use as approved by the by the CEO on behalf of the Council.

q) Ensure that when a zoom facility on a camera is being used, there is a second person present with the operator of the camera to guarantee that there is no unwarranted invasion of privacy.

r) Ensure that camera control is solely to monitor suspicious behaviour, criminal damage etc. and not to monitor individual characteristics.

s) Ensure that camera control is not infringing an individual's reasonable expectation of privacy in public areas.

16. Review

In order to ensure Council continues to provide the best possible service responses to its customers, this Policy will be subject to periodic evaluation and review.

17. History

Document History:	Version No:	Issue Date	Description of Change
	1.0	28/09/2021	Development of draft
	2.00	18/03/2025	No Amendments