SOUTH GIPPSLAND SHIRE COUNCIL

COUNCIL POLICY

South Gippsland Shire Council

ELECTRONIC SURVEILLANCE DATA USAGE POLICY

Policy No.	C89	Adoption Date:	Council Meeting 17 July 2024
Revision Date:	July 2028		
Directorate:	Performance & Innovation	Department:	Digital & Technology
GOOD GOVERNANCE FRAMEWORK – OVERARCHING PRINCIPLES			
Supporting Pillar:	Pillar 7 - Risk & Compliance		
Link to Pillar:	The Policy supports Risk & Compliance by outlining the requirements needed to meet relevant legislative requirements relating to the privacy and data protection of surveillance data.		

1. PURPOSE

1.1. The purpose of the *Electronic Surveillance Data Usage Policy (C89)* (the Policy) is to provide the appropriate framework for the implementation, installation, data management, operation, and retrieval of electronic surveillance owned and managed by South Gippsland Shire Council (Council).

1.2. This Policy has been developed in the interests of contributing to public safety and/or the protection of Council assets. The *Surveillance Devices Act 1999* and the *Privacy and Data Protection Act 2014* regulates the usage of electronic surveillance devices, including CCTV, and how this data is handled and stored.

2. SCOPE

2.1. The scope of this Policy applies to the provision of, and all users of, Council information technology services, equipment and connectivity.

2.2. Surveillance equipment can include all devices that can:

2.2.1. Identify or detect suspicious or anomalous activity on, or over, a computer network;

2.2.2. Take images, audio, or video capture for the purposes of surveillance.

2.2.3. Record and identify physical access to, movement within, or changes to a specific area, such as a building, room, or external grounds.

2.2.4. Report on geolocation/location services information.

2.3. Electronic Surveillance activities can include, but are not limited to:

2.3.1. Access Control Systems;

2.3.2. CCTV and body worn cameras;

2.3.3. Mobile devices;

2.3.4. Drones;

2.3.5. Network Intrusion Detection Systems;

2.3.6. Software logging services;

2.3.7. Duress devices/alarms

2.3.8. Other surveillance and auditing services.

3. POLICY PRINCIPLES

Intent of Surveillance Systems

3.1. The intention of surveillance systems used by Council may be to:

3.1.1. Deter crime by increasing the chance of detection.

3.1.2. Protect people and assets through active monitoring.

3.1.3. Investigate crimes that have occurred on or against Council assets or personnel.

3.1.4. Support public safety and provide support in emergencies or active threat situations.

3.1.5. Improve plant and resource efficiency.

3.1.6. Improving service responsiveness.

Types of Surveillance Systems

3.2. Council's surveillance systems may be of the following type:

3.2.1. Physical Access Control Systems (PACS)

3.2.2. Video Surveillance Systems (VSS)

3.2.3. Intrusion Detection Systems (IDS)

3.2.4. Passive monitoring services

Allowable Purposes

3.3. Council may consider the placement of either permanent or temporary Electronic Surveillance Systems for the following purposes:

3.3.1. Improving public safety, both perceived and actual, by the discouragement of unlawful activity and antisocial behaviour, in or around Council facilities, assets or public spaces;

3.3.2. To assist a Law Enforcement Agency or a Council authorised officer with the detection and prosecution of offences;

3.3.3. For the protection of Council physical and technology assets, or assets managed by Council;

3.3.4. For the identification and prevention of crime, including fraud, theft, and vandalism, both physical and electronic;

3.3.5. Monitor physical spaces and electronic systems and services where staff interact with the public, to enhance safety;

3.3.6. To enable providing of evidence and its assessment of any incident or other event that occurs at, in, or on:

i. The immediate vicinity of Council facilities;

ii. Council networks, systems, or services;

iii. When aiding in the safe operation of equipment, technology, or, work area.

3.4. Electronic Surveillance equipment or services may be temporarily installed in or on Council premises, or in public areas, for a limited amount of time where;

3.4.1. A permanent device or service may not be practicable. i.e. the cost;

3.4.2. The subject area has a sudden spike or commencement of criminal or antisocial activity, or other activities that could be detrimental to Council interests;

3.4.3. Where other security measures have failed or proved ineffective in preventing or controlling mentioned issues;

3.4.4. For the determination of whether an ongoing need or benefit for Electronic Surveillance is needed; or

3.4.5. An area that is under the short-term control of Council (e.g. event, function, building site).

3.5. Council vehicles may also have tracking devices to monitor location, activity and the safety and wellbeing of Council employees. This may include GPS location, vehicle status and duress alarms.

Approval of Surveillance Devices

3.6. The Chief Executive Officer is authorised to delegate approval of Deployment/use of all surveillance equipment and activities.

3.7. The Chief Executive Officer is authorised to delegate approval, disapproval, or cancellation of the use and/or implementation of surveillance systems or devices.

3.8. Use of Council's Electronic Surveillance Framework and Procedure will be applied for the approval and placement of surveillance equipment.

3.9. The following activities will not be approved:

3.9.1. Use of privately invasive or disproportionate technology capabilities not commensurate with the risk.

3.9.2. Surveillance devices within private spaces such as toilets, washrooms, change rooms and the like.

3.9.3. Devices that don't meet the requirements of this Policy.

3.10. Users of Council sites or properties using their own surveillance system, must comply Council's guidelines which will be outlined in a written agreement with Council. This includes management of access, extraction, disclosure, signage etc.

Signage

3.11. Where Video Surveillance Systems (VSS) are in use, appropriate signage will be displayed to indicate that the area is being recorded. Refer to attachments for approved examples.

3.11.1. Signage will comply with relevant Australian Standards and legislation, and with the following requirements:

3.11.2. Signs are to be placed at the main entry point of the surveillance areas where there is public access.

3.11.3. Signs need to be easily understood, including those who are from non-English speaking backgrounds. The signs can include a mix of text and symbols.

3.11.4. Signs need to be clearly visible, located in areas with good lighting, within normal eye range, with accessible colours, and large enough so text can be easily read.

3.11.5. Signs will clearly identify the organisation and/or owner of the system undertaking surveillance.

3.11.6. Signs will include details of who to contact for any queries about the surveillance system. If this is Council, the primary listed number will be utilised.

3.11.7. Signs will be routinely checked for damage and/or theft and replaced where required.

3.12. If an individual requests further information on the purpose, access, and disclosure of footage, they will be directed to this Policy which will be made publicly available on Council's website page.

3.12.1. Further information regarding Council's obligations to protect personal information and data can be found on Council's publicly available *Information Privacy Policy (C22)* and website privacy statement.

3.13. Once Video Surveillance Systems activities have ceased, all signage and equipment will be removed as soon as practicable.

Data Security

3.14. Data collected is not for the purpose of public access to the data, as in accordance with the intentions of this Policy.

3.15. Unless otherwise required by a Law Enforcement Agency, or by law, Electronic Surveillance data (e.g. camera footage, access logs) is temporary and will be destroyed in accordance with the *Public Records Act 1973*, unless otherwise required for legal reasons.

3.16. In general, the following retention periods will be used, unless otherwise approved by Council's Privacy & Cyber Security Board or required by law (such as an Act):

3.16.1. Video Surveillance Systems (VSS) data will be retained for up to 30 days.

3.16.2. Physical Access Control Systems (PACS) data will be retained for up to 7 years.

3.16.3. Intrusion Detection Systems (IDS) data will be retained for up to 7 years.

3.17. Data that is collected for the purposes of enforcement activities shall be securely stored in a centralised location. Evidence that is obtained and retained needs to be done so in accordance with the *Evidence Act 2008*.

3.18. Surveillance data collected is a public record, and therefore Council will need to ensure that management of these records comply with the *Public Records Act 1973*, *Surveillance Devices Act 1999* and the *Privacy and Data Protection Act 2014*.

3.19. Council can only provide or transfer ownership of data in accordance with provisions made in the *Privacy and Data Protection Act 2014* and Council's *Information Privacy Policy* (C22) or where required by law.

Victoria Police Agreement

3.20. For any public safety system, a written agreement will be in place with Victoria Police prior to implementing the system.

3.21. These agreements must cover:

3.21.1. Responsibilities of both Council and Victoria Police;

3.21.2. Ownership of the system and the data it produces;

3.21.3. Oversight and a review of the mechanisms in place, including how Council will be assured Victoria Police is using and managing information appropriately.

Logging & Monitoring

3.22. Logging is the automated collection of transaction records to provide a method of monitoring and investigating privacy and security incidents, identify potential threats, and provide a clear audit trail for the safety of staff at Council.

3.23. Maintaining logs, backups and archives of user and administrator activities on all Council technology resources including:

3.23.1. Servers, databases, desktop and laptop computers;

3.23.2. Cloud services and software providers;

3.23.3. Portable devices such as smartphones and tablets;

3.23.4. Building, facility, and room access cards and/or fobs.

3.23.5. Monitoring email, backups and archives of emails sent and received through Council email servers; and

3.23.6. Retaining logs, backups and archives of all Internet access and network usage.

3.24. Council will not disclose the contents of monitoring to a person, body, or directorate (other than the individual concerned) unless one or more of the following applies:

3.24.1. The staff member is reasonably likely to have been aware, or made aware that information of that kind is usually passed to that person, body or directorate;

3.24.2. They have consented to the disclosure;

3.24.3. There exists an actual or perceived threat where mandatory reporting to authorities is required.

Access to Data

3.25. Access and/or disclosure to any data needs to be in line with the *Privacy and Data Protection Act 2014* and Council's *Information Privacy Policy (C22).*

3.26. Access will generally be retrospective reviews; however, there may be circumstances or periods where passive monitoring will be required.

3.27. The Chief Executive Officer is authorised to delegate access to the data collected.

3.28. Access must not be through a generic or shared login.

3.29. Equipment used to capture and store surveillance data will be stored in a way that prevents the risk of unauthorised access, tampering or data theft.

3.30. An access, extraction and disclosure register shall be maintained, with each access registered as to why data was accessed and by whom. The register will be regularly reviewed by an authorised user and the Manager Digital & Technology.

3.31. Any disclosure of data shall require approval of the Manager Digital & Technology.

3.32. Any request for access to data by a third party, other than for legal purposes, is to be made through Council's Freedom of Information process.

Standard Operating Procedure

3.33. The Standard Operating Procedure (SOP) must align and be consistent with the requirements of this Policy, and must be:

3.33.1. Provided to any VSS, IDS, and PACS users and administrators.

3.33.2. Reviewed at least every two years.

3.34. The Digital & Technology Department will be responsible for providing training and information for the surveillance technology to authorised users. This includes both technical training and laws and obligations. They will also maintain:

3.34.1. Details design drawings

3.34.2. Product specifications

3.34.3. Warranty information

3.34.4. Record and data management requirements

Inappropriate Use and Complaint Handling

3.35. Council officers who are using or working with surveillance equipment are to comply with the requirements of this Policy.

3.36. Where a Council employee is in breach of this Policy, an internal review will be conducted, and appropriate actions taken in accordance with the *Employee Code of Conduct (CE20)*.

3.37. Public complaints or requests in relation to surveillance equipment can be made in writing to:

ATTN: Privacy Officer
South Gippsland Shire Council
Private Bag 4
Leongatha VIC 3953

Or via email to council@southgippsland.vic.gov.au

3.38. If a member of the public is dissatisfied with the outcome of their complaint, they also have a right to complain to the Victorian Ombudsman. If the complaint is in relation to privacy, complaints should be made to the Office of the Victorian Information Commissioner (OVIC).

4. RISK ASSESSMENT

This Policy mitigates Council's risks as described below:

People

4.1. This Policy aims to provide Council employees, contractors and volunteers with a clear understanding how surveillance / CCTV equipment will be used, and how data will be protected and stored.

Reputational

4.2. This Policy helps mitigate reputational risk by giving direction on the use of surveillance / CCTV equipment, and the handling of collected data in accordance with the *Privacy and Data Protection Act 2014*.

Financial

4.3. This Policy helps mitigate risk of inappropriate application and use of surveillance or CCTV equipment and data, which could result in legal action and associated costs/fines.

Governance

4.4. This Policy refers to and outlines relevant legislation that governs surveillance activities and the data it produces.

Safety

4.5. This Policy helps mitigate safety risks to Council employees and public by outlining the ways in which Council can install surveillance equipment. This deters antisocial activities and/or provides evidence for investigations.

5. IMPLEMENTATION STATEMENT

Human Rights Charter

5.1. This Policy has considered the *Charter of Human Rights and Responsibilities Act 2006* in its development.

Gender Equality

5.2. This Policy has considered the *Gender Equality Act 2020* in its development.

Roles and Responsibilities

5.3. Council will:

5.3.1. Ensure this Policy is made publicly available on its intranet and website.

5.3.2. Ensure that the proper approval, risk and training considerations are in place before approving the use of surveillance equipment.

6. MONITORING, EVALUATION AND REVIEW

6.1. This Policy will be reviewed and adopted by Council on a four-year cycle.

6.2. Prior to adoption, Council consulted with various teams and committees to gain feedback and acceptance of the policy contents. This includes Staff Consultative Committee, Executive Leadership Group and Audit and Risk Committee.

7. REFERENCE DOCUMENTS

Legislative Provisions	Charter of Human Rights and Responsibilities Act 2006 Evidence Act 2008 Freedom of Information Act 1982 Local Government Act 1989 Local Government Act 2020 Occupational Health and Safety Act 2004 Privacy and Data Protection Act 2014 Public Records Act 1973 Private Security Act 2004 Surveillance Devices Act 1999
Council Supporting Documents	Information Privacy Policy (C22) IT Acceptable Use Policy (CE99) Employee Code of Conduct (CE20) Corporate Information Management Policy (CE49) Motor Vehicle Policy (CE12)

8. DEFINITIONS

Authorised User	A Council system user who has permission to access certain databases.
Body Worn Cameras	A wearable audio, video or photographic recording system.
CCTV System	'Closed Circuit Television system' is a form of video surveillance technology.
FOI	Freedom of Information, usually used in relation to a Freedom of Information Request, a request made under the *Freedom of Information Act 1982* which allows your right to request access to government held information.
Intrusion Detection Systems (IDS)	Monitors network traffic and reports suspicious activity to incident response teams.
Live monitoring	Where surveillance monitors or smart phones are intermittently observed by operators.
Passive Monitoring	A process where data or information is collected without interaction with the system. Includes continuous of periodic observation and recording of activities.
Physical Access Control Systems (PACS)	Restricts who can access a physical space, usually consisting of a barrier, a reader, credentials, control panel and server.
Public Safety System	Surveillance activities set up to protect safety in public spaces.
Retrospective review	Where surveillance is reviewed after an incident.
Surveillance Device	Equipment that is capable of collecting, capturing, recording, retaining and processing audio, video, photographic, logs etc.
Temporary cameras	Cameras that are not permanently placed in a location and can be moved. Examples could include trail cameras that temporarily capture the movement of animals in a location.
Video Surveillance Systems (VSS)	Also known as CCTV, visual monitoring system using cameras or other devices to record video or images.

9. REVISION HISTORY

Approved By	Approval Date	Sections Modified	CM9 Ref#
Council	*17 July 2024*	*New Policy*	*D8308522*

10. ATTACHMENTS

10.1. Example signage one:

10.2. Example signage two