

Surveillance Devices Policy

Version 2.1

March 2025

1 Purpose and Scope

The NSW State Emergency Service (NSW SES) uses surveillance technology as an enhancement tool for operations and the business functions of NSW SES.

The use of surveillance technology results in NSW SES collecting Personal Information. This includes the location of individuals and, depending on the type of technology, what individuals are doing or saying at the time the Personal Information is collected. The use of Surveillance Devices in these circumstances is justified and necessary for operational reasons and to support the business functions of NSW SES.

It is essential that NSW SES has real time information about the location of members and others involved in NSW SES operations to ensure their safety. Outside of operations, it is also important that NSW SES is able to protect the infrastructure that allows NSW SES to be effective in operations. In general, other Surveillance Data that is collected is used in limited circumstances for purposes where required or authorised by law.

This policy has been developed for:

- NSW SES members;
- individuals who may be involved in NSW SES operations;
- visitors to NSW SES premises (including mobile SES premises); and
- suppliers and service providers and their employees,

whose Personal Information may be collected as a result of NSW SES Surveillance Devices. It also covers any Personal Information collected through the use of approved software or applications where NSW SES members bring their own device (BYOD).

The purpose of this policy is to clarify:

- key principles for use of surveillance technology by NSW SES;
- the types of surveillance technology used by NSW SES;
- the kinds of Personal Information that may be collected;
- when and how NSW SES will use this Personal Information;
- when and how NSW SES will disclose this Personal Information;
- how long NSW SES will store this Personal Information; and
- rights to access this Personal Information.

2 Policy principles for the collection and use of Surveillance Data

2.1 Key principles

The standards and legislative principles underpinning this Policy are:

A. Authorised programs will be the primary use case for surveillance technology

Surveillance technology will primarily be used by members as part of coordinated programs that address significant risks, inefficiencies or capability gaps. These programs will be developed by Program Leads in consultation with the Surveillance Devices Policy Owner and other relevant stakeholders and approved by the Policy Sponsor. On a case-by-case basis, the Policy Sponsor may authorise short term use of Surveillance Devices outside of a program (e.g. a small trial).

Unless specifically directed, NSW SES does not authorise its members to use the surveillance functions of their own devices as part of their duties.

B. Use of technology and data must only be for approved purposes

NSW SES will only use Surveillance Devices to collect, use or disclose Surveillance Data if these activities will be:

- for a purpose that is legitimate and related to the employment/engagement of members or the business activities or functions of NSW SES. Specifically:

as an enhancement tool for operations and the business functions of NSW SES that allows for:

- *improved safety of members and others involved in NSW SES operations*
- *securing a known locality*
- *better dispatch and management of NSW SES assets and members through improved information gathering*
- *the security of NSW SES buildings and equipment and/or data*
- *performance of its functions as set out in the SES Act and State Emergency and Rescue Management Act 1989 (NSW)*
- *debriefing and training of members, and*
- *improved interoperability with other Emergency Service Organisations.*

NSW SES uses Surveillance Data for these approved purposes and directly related (secondary) purposes that support its operations and business functions.

- disclosure to a law enforcement agency in connection with the detection, investigation or prosecution of an offence
- related to the starting or continuation of civil or criminal legal proceedings
- necessary to avert an imminent threat of serious violence (or in the case of Personal Information, threat to life and health) or substantial damage to property, and
- as permitted or authorised by privacy or other laws.

The purpose that a device is approved for must be central to all decisions about use of device and handling of Surveillance Data.

C. NSW SES will notify members and others of Surveillance Device use

If members may be observed through a Surveillance Device, written notices will be issued to members outlining specific information about the surveillance program. This notice will be issued as part of induction or 14 days in advance of a new program starting.

In-application alerts or log-on banners may also be used for software applications downloaded on a mobile or other computing device.

Privacy collection notices will be issued or updated (if required) if Personal Information or Health Information will be collected. These notices must outline the purpose for collection and how data will be used, disclosed and stored.

Signage will be in place at entrances and prominent areas if Optical or Tracking will be used in relation to NSW SES vehicles or devices/equipment or at usual NSW SES premises. The devices or casings used for Optical or Tracking devices must be clearly visible. Signage will be in place at each entrance to the State Operations Centre (SOC) for call recording.

D. Members should only have the access necessary to conduct their roles

Access to and use of Surveillance Data will be controlled and limited on a need to know basis. Access permissions to Surveillance Devices, settings and Surveillance Data will be set by the Program Lead in consultation with the Policy Owner and Policy Sponsor. These will include different levels of access according to need.

Generally, Surveillance Data will be viewed in limited and controlled settings. If access is granted to a wide group (e.g., through Beacon), then the information to be displayed will be as limited and anonymised as possible.

Certain types of information should not be shared outside of closely controlled settings (e.g., private conversations or treatment of injured persons).

E. Surveillance Data will be securely managed in accordance with legal and policy requirements

As the data is likely to contain Personal Information it must:

- only be kept for the purpose for which it may be lawfully used for business, legal and accountability requirements and no longer than necessary for that purpose (which may be impacted by retention periods under the State Records Act)
- be protected from unauthorised access, use, modification and disclosure
- only be disclosed if a NSW SES member trained in relevant laws has determined it is lawful to do so and then, only disclosed to the extent necessary, and
- be retained and disposed of in accordance with State Records requirements.

NSW SES will seek to ensure the integrity of data throughout processes for upload, storage, retrieval and disposal processes.

F. Surveillance Device programs will be monitored and evaluated

Surveillance programs must be developed so that NSW SES will be able to readily monitor and evaluate its activities for effectiveness against the purpose of the program and compliance with procedural requirements.

2.2 Prohibited purposes for the collection and use of Surveillance Data

A Surveillance Device must not be used in a way that is inconsistent with the authority or directions of NSW SES. The Procedure sets out prohibited purposes for use of a Surveillance Device to collect and use of Surveillance Data.

2.3 The types of surveillance technology used by NSW SES

The types of surveillance technology used by NSW SES comprises a broad range of Surveillance Devices including Tracking Devices, Optical Surveillance Devices, Data Surveillance and, in limited instances, Listening Devices. These devices may capture images, location information, audio and activity records. Examples include personal locator beacons, GPS, mobile phones (whether BYOD or NSW SES supplied), fixed, portable or mobile radio, computer surveillance, CCTV and telematics in NSW SES fleet vehicles.

NSW SES has determined that the use of these technologies is necessary for operations and to support the business functions of NSW SES. **By continuing as a member of NSW SES, members consent to the use of these Surveillance Devices as described in this policy. Individuals who are not NSW SES members but who engage with NSW SES in operations or for business purposes are also required to consent to the use of Surveillance Devices. Program planning must ensure appropriate steps are taken to provide notification and obtain consent for each authorised program.**

2.4 The kinds of Personal Information collected using Surveillance Devices

Surveillance Devices will capture information that may include Personal Information. The kinds of Personal Information that can be collected using Surveillance Devices includes:

- for Tracking Devices: an individual's location and movements over a period of time.
- for Optical Surveillance Devices: an individual's location and what the individual was doing at that time.
- for Data Surveillance Devices: Data Surveillance Devices often comprise apps or programs that are installed on a computer or other device to allow the surveillance of any data that is entered on the device. The data collected may include an individual's location and driving behaviour (for Telematic devices) and opinions and views expressed by individuals (for other devices). These devices will also record data that is not Personal Information.
- for Listening Devices: an individual's location and statements made or opinions expressed by the individual at that time.

2.5 When and how NSW SES uses this Surveillance Data

2.5.1 How NSW SES uses Surveillance Data

How NSW SES uses Surveillance Data collected using surveillance technology varies according to the nature of the information collected and its relevance to operations and the business functions of NSW SES. Annexure A contains examples of current uses of Surveillance Data by different NSW SES directorates.

2.5.2 Tracking Devices

The use of Tracking Devices and at least some of the Surveillance Data collected by NSW SES is directly related to NSW SES operations. For example, in the event of an emergency, having equipment that is fitted with a Tracking Device will support member safety by allowing a more effective response to a distress signal. While the use of Tracking Devices may result in the collection of Surveillance Data that is not required for operations, that Surveillance Data is only used in limited circumstances for other purposes where required or authorised by law.

SES members may be tagged on Tracking Devices. When Personal Information is collected by NSW SES using Surveillance Devices other than Tracking Devices, the individual may be identifiable (for example by their voice or image) but they are not tagged.

2.5.3 Surveillance outside of operations

If you take NSW SES issued equipment home with you that has been fitted with a Tracking Device, it may continue to track the location of the equipment. This may include your location if you are carrying the equipment with you and the tracking functionality is enabled. If the Tracking Device was switched off while the equipment is not being used for operations, there is a risk of the Tracking Device not being switched back on and an individual not being able to be located readily if they issue a distress signal subsequently. NSW SES believes this risk outweighs the risk of interference with an individual's privacy while the equipment is not being used for operations.

2.5.4 Audio recordings

The use of devices that can monitor or record conversations are covered by several statutes to ensure private conversations (including through calls) are not inappropriately recorded, stored, listened to or communicated. NSW SES utilises audio recording in limited and controlled circumstances.

These circumstances include:

- Radio talk groups which are recorded for quality assurance to ensure that members are meeting requisite standards and for educational purposes, for records management, and member safety (e.g. console instant recall); and
- Calls to the State Operations Centre (SOC) by members of the public contacting NSW SES to request assistance, as well as calls made from the SOC or within the SOC. These recordings are used in after action reviews. The recording of these calls is strictly managed in accordance with the *Telecommunications (Interception and Access) Act 1979* (Cth).

2.5.5 Security of NSW SES buildings and equipment

Surveillance Devices and Surveillance Data are used by NSW SES to maintain security of NSW SES buildings and equipment and/or data.

In the case of NSW SES buildings, NSW SES may use Surveillance Data in real time to protect the buildings from unauthorised access or negligent or malicious damage. NSW SES may also use Surveillance Data to investigate unauthorised access or negligent or malicious damage to a building. In addition to this, the Building Owner may maintain CCTV coverage of public and shared areas e.g. parking areas and thoroughfares.

In the case of NSW SES equipment, NSW SES may use Surveillance Data to locate and recover equipment. NSW SES may also use Surveillance Data to investigate negligent or malicious damage to equipment.

In the case of NSW SES data, NSW SES may use Surveillance Data or prevent the negligent or malicious use of or damage to agency held data.

2.5.6 Other uses of Surveillance Data

With limited exceptions, Surveillance Data is not recorded in a file that is specific to a NSW SES member or other individual. Records of incident management and response are classified as State Records and are likely to include Surveillance Data collected by Tracking Devices. Because NSW SES does not record Surveillance Data in individual files, there are limited other uses for that Personal Information.

Other uses include investigating grievances, disciplinary or misconduct matters concerning a NSW SES member if the relevant incident may have been recorded using a Surveillance Device.

2.6 Determining access and use permissions to Surveillance Data

For each type of Surveillance Device used by NSW SES, appropriate access permissions will be determined and documented to ensure that Surveillance Data is only used for the purposes stated in 2.5.

This includes assessing the information that may be collected, how that will be accessed, and which NSW SES members require access to perform their functions.

2.7 When NSW SES discloses Personal Information

In general, Surveillance Data collected by NSW SES is not disclosed to third parties. The general requirements that apply when disclosure is considered are described below and specific disclosure circumstances are described in the Procedure.

2.7.1 Disclosure to other Emergency Services Organisations

NSW SES works with other Emergency Services Organisations (**ESOs**). Section 27D of the PPIPA (*Privacy and Personal Information Protection Act 1998 NSW*) permits the disclosure of Personal Information if the disclosure is reasonably necessary to assist in a stage of an emergency. The type of Personal Information that NSW SES is likely to disclose to another ESO is limited to an individual's location, NSW SES equipment they have available to them and their experience.

2.7.2 Disclosure to protect individuals

Under the PPIPA disclosure of Personal Information is permitted if the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person. A similar standard applies under the *Workplace Surveillance Act and Surveillance Devices Act*, which permit disclosure to avert an imminent threat of violence.

2.7.3 Disclosure to protect NSW SES buildings and equipment

If NSW SES has Surveillance Data of unauthorised access or negligent or malicious damage to a building, equipment or agency held data, it may disclose that information to third parties to protect that building, equipment or data including the police for law enforcement purposes.

2.7.4 Disclosure authorised or required by law

Various laws require or authorise the disclosure of Personal Information in limited circumstances. Examples include information that may be required by the police in a criminal investigation or if NSW SES is involved in a coronial enquiry. In these circumstances NSW SES always seeks to limit the disclosure to the extent necessary or required to comply with the relevant law.

2.8 How long does NSW SES store this Personal Information

2.8.1 Retention and disposal authorities

NSW SES is subject to GA28 General Retention and Disposal Authority: Administrative Records and FA0359 Functional Retention and Disposal Authority. Each authority governs how long certain records are required to be retained by the NSW SES. These records may contain Personal Information. It is unlikely that any Personal Information contained in these records will be stored separate to those records.

2.8.2 State Records

Depending on the classification of the incident to which the information relates, records of incidents may be classified as State Records that are required to be archived (and kept indefinitely) or kept for minimum periods ranging from 2 years to 15 years after the relevant action has been completed. In some cases, State Records are only required to be kept until the administrative or reference use is no longer required by NSW SES. After the expiry of the minimum period, they may be destroyed. During the minimum retention period, NSW SES must maintain the security of these State Records.

2.8.3 Surveillance Data not comprising State Records

Surveillance Data that is collected to maintain the security of NSW SES buildings and equipment ordinarily will not comprise a State Record unless required for evidentiary, regulatory or other operational purposes. Surveillance Data that is collected to maintain the security of NSW SES buildings, equipment and data that is used by NSW SES for law enforcement purposes or some other purpose permitted or authorised under the PPIPA will be retained by NSW SES in accordance with the PPIPA and/or the State Records Act.

2.9 Rights to access Personal Information

Under the PPIPA, individuals have the right to access personal information held by agencies including the NSW SES.

NSW SES may not be aware that it is holding Personal Information about an individual if that information has been collected using a Surveillance Device.

On request, NSW SES may be able to confirm whether it holds Personal Information about an individual if the individual is able to identify the date and time when the information may have been collected and means of collection. If NSW SES confirms that it holds Personal Information about an individual, it will provide the individual with access to that information in accordance with its obligations under the PPIPA.

3 Related Documents

Related NSW SES policies and procedures include:

- Code of Conduct and Ethics
- Dealing with Allegations of Misconduct – Volunteer members
- Distress Beacon and Radio Duress Policy and Procedure

- External Complaints Policy
- ICT Acceptable Use Policy
- ICT User Access Policy
- Cyber Security Policy
- Internal Grievances Policy
- Mobile Devices Policy
- Privacy Collection Notice – employee and volunteer members (2023)
- Privacy Management Plan
- Records Management Policy and Guideline

Related legislation and external documents include:

- *Government Information (Public Access) Act 2009* (NSW)
- Information Privacy Commission NSW, Fact Sheet: Managing access to audio visual information under the GIPA Act
- Policy Statement and Guidelines for the establishment and implementation of CCTV in public places (Department of Justice 2014)
- NSW State Rescue Policy (4th Edition, 2021)
- NSW Treasury Telematics Policy
- *Privacy and Personal Information Protection Act 1998* (NSW)
- *Security Industry Act 1997* (NSW)
- *State Records Act 1998* (NSW), General Retention and Disposal Authority GA 28, Functional Retention and Disposal Authority: FA359
- *Surveillance Devices Act 2007* (NSW)
- *Telecommunications (Interception and Access) Act 1979* (Cth)
- *Workplace Surveillance Act 2005* (NSW)
- *Government Sector Employment Act 2013* (NSW)

4 Support and Advice

You can get advice and support about anything in this policy from:

- your Manager or Zone Commander
- the Policy Owner
- the Policy Sponsor

5 Definitions

Term	Definition
Authorised Member	a member of NSW SES authorised as part of a program to access and operate the Surveillance Device, configure any adjustable settings and/or see live or static data.
Key Principle	the key principles for NSW SES use of Surveillance Devices and Data set out in the Policy including: A: Authorised programs will be the primary use case for surveillance technology B: Use of technology and data must only be for approved purposes C: NSW SES will notify members and others of Surveillance Device use D: Members should only have access necessary to conduct their roles E: Surveillance Data will be securely managed in accordance with legal and policy requirements F: Surveillance Device programs will be monitored and evaluated.
Data Surveillance Device or Data Device	any device or program capable of being used to record or monitor the input of information into or output of information from a computer, but does not include an optical surveillance device. Data Surveillance Devices include computer surveillance devices and devices that use Telematics technology.
Listening Device	any device capable of being used to overhear, record, monitor or listen to a conversation or words spoken to or by any person in conversation, but does not include a hearing aid or similar device used by a person with impaired hearing to overcome the impairment and permit that person to hear only sounds ordinarily audible to the human ear. Listening Devices include voice recorders and any device that has a listening device function like a mobile phone or laptop.
Optical Surveillance Device or Optical Device	any device capable of being used to record visually or observe an activity, but does not include spectacles, contact lenses or a similar device used by a person with impaired sight to overcome that impairment. Optical Surveillance Devices include cameras and any device that has a camera function like a mobile phone or laptop. CCTV is an Optical Surveillance Device.
Personal Information	information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.
PPIPA	<i>Privacy and Personal Information Protection Act 1998 (NSW).</i>

Term	Definition
Authorised Program	An approved use of Surveillance information, managed by the Program Lead
Program Lead	the member of NSW SES that is responsible for the development, management and review of a program to use a particular Surveillance Device for an approved purpose.
Program guidelines	guidelines developed to provide direction to members on implementation of a particular program.
State Records	any record made and kept, or received and kept, by any person in the course of the exercise of official functions in a public office, or for any purpose of a public office, or for the use of public office.
State Records Act	<i>State Records Act 1998</i> (NSW).
Surveillance Device	(a) a Data Surveillance Device, a Listening Device, an Optical Surveillance Device or a Tracking Device, or (b) a device that is a combination of any 2 or more of the devices referred to in paragraph (a).
Surveillance Data	data including Personal Information obtained, recorded, monitored or observed by a Surveillance Device.
Telematics	technology that uses a device attached to a vehicle to gather data including vehicle location, driver behaviour and vehicle activity.
Tracking Device	any electronic device capable of being used to determine or monitor the geographical location of a person or an object. Tracking Devices include any device that has a tracking function like a mobile phone or laptop.

Annexure A: NSW SES Directorates – dealing with Surveillance Data

These are examples of current uses of Surveillance Data that may occur. Each use of a Surveillance Device is subject to this policy and related procedures.

Directorate	Example Uses of Surveillance Data
Operations (Metro and South & North and West)	- Receiving and responding to Requests for Assistance. - Coordination with other agencies. - Volunteer member management. - Investigations of grievances and disciplinary matters.
Emergency Management	- Audio recording information from callers to the 132 500 number within State Operations Centre. - Recording of calls across the business at a state and local level in line with legislative requirements. - Project work involving stakeholder engagement. - Database entry, administration, extraction and storage (Beacon).
Operational Capability and Training	Training purposes.
People and Development	- Investigations of grievances and disciplinary matters involving staff members and/or volunteer members. - Investigating serious allegations against staff members and/or volunteer members including serious misconduct or breaches of discipline, corruption, potential criminal and other high-risk matters.
Information and Communications Technology	- ICT records, including records of external access to NSW SES websites. - Database entry, administration, extraction and storage (including Power BI).
Finance, Asset and Business Services	- CCTV recordings from security cameras. - Collection of personal information through the Kiosk facility at SHQ reception, which is used to sign people into the building, and similar functions at other NSW SES premises.
Other Directorates (Organisational Strategy, Planning & Performance, Media & Communications, Office of the Commissioner)	- Dealing with access applications under the <i>Government Information (Public Access) Act 2009</i> (NSW). - Dealing with complaints and requests for internal review under the PPIPA and <i>Health Records and Information Privacy Act 2002</i> (NSW). - Responding to subpoenas and other lawful orders to produce.

Document Control Sheet

Title	Surveillance Devices Policy
Current Version	2.1
Directorate	Organisational Strategy, Planning and Performance
Policy Owner	Director Organisational Strategy, Planning and Performance
Policy Sponsor	Deputy Commissioner Corporate Services
Effective date	19/01/2024
Next Review Date	19/01/2029
Rescinds	Surveillance Devices Policy v2.0
Topic	Security
Function	ICT, Information Management
Key Words	Surveillance

Version History

Version #	Creation Date	Author	Summary of changes
1.0	03/09/2017		Final
2.0	19/12/2023		Full review and document name change
2.1	19/03/2025	Policy Team	Administrative update – reference to related document <i>Information Security Policy</i> changed to <i>Cyber Security Policy</i> .

Approval

Title		Date	Version signed off
Director Organisational Strategy, Planning and Performance	Policy Owner	21/12/2023	v2.0
Deputy Commissioner Corporate Services	Policy Sponsor	22/12/2023	v2.0
Carlene York	Commissioner	22/12/2023	v2.0