Privacy Management Plan

2 December 2022

Table of Contents

Introduction

The NSW State Emergency Service (NSW SES) is a public sector agency that has obligations under the *Privacy and Personal Information Protection Act 1998* (NSW) (PPIPA) and the *Health Records and Information Privacy Act 2002* (NSW) (HRIPA).

The NSW SES is required to prepare and implement a Privacy Management Plan (plan) in accordance with section 33 of the PPIPA.

This plan outlines the NSW SES's practices and procedures in handling personal information under the PPIPA and health information under the HRIPA and sets out the NSW SES' commitment to respecting the privacy rights of its members. This plan will be reviewed regularly to ensure any legislative, administrative or systemic changes are reflected in this Plan.

1 Legislation

1.1 *Privacy and Personal Information Protection Act 1998* (NSW) (PPIPA)

The PPIPA outlines how the NSW SES must manage personal information. It also outlines the functions of the Privacy Commissioner. While the PPIPA recognises a person's right to privacy, that right is not absolute. The PPIPA provides a number of exemptions and exceptions to the privacy principles.

The PPIPA protects your personal information by:

- making sure that your personal information is properly collected, stored, used or released in accordance with Information Protection Principles (IPPs),
- giving you the right to see and ask for changes to be made to your personal information,
- allowing you to make a complaint to the NSW Privacy Commissioner if you believe a NSW public sector agency has misused your personal information or breached one of the IPPs.

Definition of personal information

The legal definition of personal information is provided in section 4 of the PPIPA. Section 4 of the PPIPA defines 'personal information' as:

> *"Information or an opinion (including information or an opinion forming part of a database and whether or not in a recorded form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion".*

Personal information includes such things as a person's fingerprints, retina prints, body samples or genetic characteristics.

As an example, personal information can be considered to be information that identifies you. Personal information can include:

- a record which may include your name, address and other details about you,
- photographs, images, video or audio footage,
- fingerprints, blood or DNA samples.

There are some kinds of information that are not personal information, e.g. information about someone who has been dead for more than 30 years, information about someone that is contained in a publicly available publication, or information or an opinion about a person's suitability for employment as a public sector official. Health information is generally excluded here as it is covered by the HRIPA.

When is personal information 'held' by the NSW SES

Personal information is held by the NSW SES if:

- it possesses or controls the information; or
- the information is in the possession or control of a person employed or engaged by the NSW SES in the course of their employment/membership; or
- the information is contained in a state record in respect of which the agency is responsible under the *State Records Act 1998* (NSW).

The Information Protection Principles under PPIPA

The 12 IPPs are the key to the PPIPA. They are legal duties that describe what the NSW SES must do when it handles your personal information. The IPPs detail how your personal information must be collected, stored, used and disclosed as well as your rights to access and correct your personal information.

These are the 12 IPPs:

<u>Collection</u>

- **IPP 1 (Lawful)**: only collect personal information for a lawful purpose, which is directly related to the agency's function or activities necessary for that purpose.
- **IPP 2 (Direct)**: only collect personal information directly from the person concerned, unless they have authorised collection from someone else, or if the person is under the age of 16 and the information has been provided by a parent or guardian.
- **IPP 3 (Open)**: inform the person you are collecting the information from why you are collecting it, what you do with it and who else might see it. Tell the person how they can view and correct their personal information, if the information is required by law or voluntary, and any consequences that may apply if they decide not to provide their information.
- **IPP 4 (Relevant)**: ensure that the personal information is relevant, accurate, complete, up-to-date and not excessive and that the collect does not unreasonably intrude into the personal affairs of the person.

Storage

- **IPP 5 (Secure)**: store personal information securely, keep it no longer than necessary and dispose of it appropriately. It should also be protected from unauthorised access, use, modification or disclosure.

Access and Accuracy

- **IPP 6 (Transparent)**: explain to the person what personal information about them is being stored, why it is being used and any rights they have to access it.

- **IPP 7 (Accessible)**: allow people to access their personal information without excessive delay or expense.

- **IPP 8 (Correct)**: allow people to update, correct or amend their personal information when necessary.

Use

- **IPP 9 (Accurate)**: make sure the personal information is relevant, accurate, up-to-date and complete before using it.

- **IPP 10 (Limited)**: only use personal information for the purpose it was collected unless the person has given their consent, or the purpose of use is directly related to the purpose for which it was collected, or to prevent or lessen a serious or imminent threat to any person's health or safety.

Disclosure

- **IPP 11 (Restricted)**: only disclose personal information with a person's consent or if the person was told at the time that it would be disclosed, if disclosure is directly related to the purpose for which the information was collected and there is no reason to believe the person would object, or the person has been made aware that information of that kind is usually disclosed, or if disclosure is necessary to prevent a serious or imminent threat to any person's health or safety.

- **IPP 12 (Safeguarded)**: an agency cannot disclose sensitive personal information without a person's consent, for example, information about ethnic or racial origin, political opinions, religious or philosophical beliefs, sexual activities, or trade union membership. It can only disclose sensitive information without consent in order to deal with a serious and imminent threat to any person' health or safety.

1.2 *Health Records and Information Privacy Act 2002* (NSW) (HRIPA)

The HRIPA outlines how the NSW SES must manage the health information of its members and the public. The HRIPA promotes the responsible handling of health information and to ensure that the protection of a person's privacy is balanced with the public interest in the legitimate use of health information.

The HRIPA protects your health information by:

- making sure that your health information is properly collected, stored, used or released in accordance with the Health Privacy Principles (HPPs),

- giving you the right to see and ask for changes to be made to your health information,

- allows you to make a complaint to the NSW Privacy Commissioner if you believe a NSW public sector agency has misused your health information or breached one of the HPPs.

Definition of health information

The legal definition of health information is provided in section 6 of the HRIPA. Section 6 of the HRIPA defines 'health information' as personal information that is information or an opinion about:

- the physical or mental health or a disability (at any time) of a person, or
- a person's express wishes about the provision of health services to him or her, or
- a health service provided, or to be provided, to a person.

Other personal information collected in relation to a provision of a health service, donation of body parts, organs or body substances and genetic information about a person arising from a health service provided to the person in a form that is or could be predictive of the health (at any time) of the person or a genetic relative of the person is included in the definition.

When is health information 'held' by the NSW SES

Health information is held by the NSW SES if:

- it possesses or controls the information; or
- the information is in the possession or control of a person employed or engaged by the NSW SES in the course of their employment/membership; or
- the information is contained in a state record in respect of which the agency is responsible under the *State Records Act 1998* (NSW).

The Health Privacy Principles under HRIPA

The 15 HPPs are the key to the HRIPA. They are legal duties that describe what the NSW SES must do when it handles your health information. The HPPs detail how your health information must be collected, stored, used and disclosed.

These are the 15 HPPs:

<u>Collection</u>

- **HPP 1 (Lawful)**: only collect your health information for a lawful purpose, which is directly related to the agency's function or activities necessary for that purpose.
- **HPP 2 (Relevant)**: ensure that your health information is relevant, accurate, up-to-date, and not excessive. The collection should not unreasonably intrude into your personal affairs.

- **HPP 3 (Direct)**: must collect your health information directly from you unless it is unreasonable or impracticable to do so.

- **HPP 4 (Open)**: must inform you of why your health information is being collected, what will be done with it and who else might access it. You must also be told how you can access and correct your health information, and any consequences if you decide not to provide it.

Storage

- **HPP 5 (Secure)**: must store your personal information securely, keep it no longer than necessary and dispose of it appropriately. It should also be protected from unauthorised access, use or disclosure.

Access and Accuracy

- **HPP 6 (Transparent)**: must provide you with details regarding the health information being stored, why it is being stored and what rights you have to access it.

- **HPP 7 (Accessible)**: must allow you access to your health information without unreasonable delay or expense.

- **HPP 8 (Correct)**: allow a person to update, correct or amend their personal information where necessary.

- **HPP 9 (Accurate)**: ensures that the health information is relevant and accurate before being used.

Use

- **HPP 10 (Limited)**: only use your health information for the purpose for which it was collected or a directly related person that you would expect (unless an exemption applies). Otherwise separate consent is required.

Disclosure

- **HPP 11 (Limited)**: only disclose your health information for the purpose for which it was collected or a directly related purpose that you would expect (unless an exemption applies). Otherwise separate consent is required.

Identifiers and anonymity

- **HPP 12 (Not identified)**: can only give you an identification number if it is reasonably necessary to carry out the agency's functions efficiently.

- **HPP 13 (Anonymous)**: give the person the option of receiving the services anonymously, where this is lawful and practical.

Transferral and linkage

- **HPP 14 (Controlled)**: only transfer health information outside NSW in accordance with HRIPA.

- **HPP 15 (Authorised)**: only use health records linkage systems if the person has provided or expressed their consent.

2 The functions and structure of the NSW SES

NSW SES is an emergency and rescue service dedicated to assisting the community. The NSW SES is a volunteer-based government organisation that provides emergency assistance to the people of NSW.

The core functions of the NSW SES are set out in section 8 of the *State Emergency Service Act 1989* (NSW) (SES Act):

- protect persons from dangers to their safety and health and protect property from destruction or damage, arising from floods, storms and tsunamis,
- act as the combat agency for dealing with floods, storms and tsunamis and to co-ordinate the evacuation and welfare of affected communities,
- assist other NSW emergency service agencies in dealing with any incident or emergency.

The NSW SES is comprised of the NSW SES Commissioner, salaried staff and volunteer members. The NSW SES has over 10,000 volunteers.

While the core function of the NSW SES is to be the combat agency for flood, storm and tsunami, the NSW SES is also involved in community safety activities. These include:

- providing advice relating to preparing for flood, storm, tsunami,
- attending properties to assist with requests for assistance,
- carrying out rescue operations allocated by the State Rescue Board,
- conducting community engagement and education programs,
- assisting the State Emergency Operations Controller in carrying out emergency management functions under the *State Emergency and Rescue Management Act 1989* (NSW),
- assisting agencies in dealing with any incident or emergency under the State Emergency Plan (EMPLAN),
- issuing flood, storm and tsunami warnings to community members at risk, including evacuation warnings and orders.

NSW SES volunteer members fulfil the core combat roles of the NSW SES, including community safety activities. Salaried staff are employed to manage the day-to-day operations of the NSW SES at State Headquarters and Zone Headquarters.

The NSW SES comprises the following Directorates:

- Metro Operations
- Regional Operations

- Operational Capability and Training
- People and Development
- Information and Communications Technology
- Finance, Asset and Business Services
- Organisational Strategy, Planning and Performance

The Commissioner is supported by the Office of the Commissioner, the Deputy Commissioner is supported by the Office of the Deputy Commissioner and Corporate Services is additionally supported by Media and Communications.

3 Types of personal and health information we collect and hold

3.1 Members of the NSW SES (Staff and Volunteers)

The NSW SES collects and holds a large amount of personal and health information about its members. Members include employees and volunteers. The information includes:

- personal contact details and emergency contact details (including telephone number, postal and email address)
- date of birth
- financial information (such as salary, bank account information, tax file number)
- personnel information (such as attendance records, leave balances, educational and professional qualifications, training records)
- background information (such as criminal history, ethnic background, disability)
- health information (including medical certificates, reports and files, and fitness for duty assessments)
- statements and opinions about operational matters
- audio recordings of telephone conversations and interviews with you (e.g. recordings of calls requesting assistance)
- photographs/footage of you in connection with your role with the NSW SES
- injury management information such as workplace injuries, workers compensation claims and payments and return to work plans
- secondary employment
- conflicts of interest
- location data (e.g. from automatic vehicle locator tracking devices used in NSW SES vehicles in accordance with NSW SES policy)
- criminal background checks which we conduct with your consent

3.2 Members of the public

The NSW SES also holds personal and health information about its customers, clients and other members of the public. Some examples of the main types of personal and health information held by clients and other members of the public include:

- name and personal contact details (including telephone number, postal and email address)
- financial information (such as bank account information)
- date of birth
- audio recordings (where incoming telephone conversations to our call centres are recorded)
- opinions (general enquiries, consultation, feedback and complaints)
- photographs/CCTV footage

4 Dealing with personal and health information

Each of the NSW SES directorates deals with personal information on a regular basis. The table below summarises the functions and the primary dealings with personal and/or health information held and managed by each directorate.

NSW SES Directorates – Functions and dealing with personal and health information

Directorate	Functions	Primary dealings with personal and/or health information
Metro Operations	Metro Operations leads and manages the strategic and operational emergency service delivery within the NSW metropolitan zone. Metro Operations comprises the following areas: <u>Zone Commander Metro</u> • Operations Readiness and Planning <u>Planning and Engagement</u> • Community Capability and Planning <u>GIS</u> • Geospatial Intelligence System Mapping <u>State Operations</u> • State Command Centre • State Operations Centre <u>Hawkesbury Nepean</u> • Hawkesbury-Nepean Valley Flood Strategy	• Receiving requests for assistance through the Communications Centre at the State Operations Centre (SOC). • Receiving Safehold information at the SOC. • Receiving and responding to Requests for Assistance. • Receiving information through ICEMS at the SOC. • Providing input to floodplain and coastal risk management issues. • Community engagement strategies, initiatives, and programs. • Audio recording information from callers to the 132 500 number. • Recording of calls across the business at a state and local level in line with legislative requirements • Providing advice to other agencies. • Volunteer management, including (but not limited to) collection, retention and use of records of volunteers' personal information. • Investigations of grievances and disciplinary matters (particularly where the investigations involve the collection of evidence from internal and external witnesses). • Project work involving stakeholder engagement. • Database entry, administration, extraction and storage (Beacon).
Regional Operations	Regional Operations leads and manages the strategic and operational emergency service delivery within NSW regional zones.	• Receiving and responding to Requests for Assistance. • Providing input to floodplain and coastal risk management issues.

Directorate	Functions	Primary dealings with personal and/or health information
	Regional Operations comprises the following areas: <u>Zone Commander (Western, North Western, Northern, North Eastern, Southern, South Eastern)</u> • Operations Readiness and Planning <u>Planning and Engagement</u> • Community Capability and Planning	• Community engagement strategies, initiatives, and programs. • Providing advice to other agencies. • Volunteer management, including (but not limited to) collection, retention and use of records of volunteers' personal information. • Investigations of grievances and disciplinary matters (particularly where the investigations involve the collection of evidence from internal and external witnesses). • Project work involving stakeholder engagement.
Operational Capability and Training	Operational Capability and Training (OCT) leads the development and planning for a range of operational capability functions of the NSW SES. OCT comprises the following areas: <u>Operational Leadership and Training Development</u> • Operational Leadership • Program Design <u>Capability</u> • Operational Improvement and Lessons • Capability • Planning and Warnings <u>Training Systems and Quality Assurance</u> • Training Systems and Quality Assurance	• Collection of staff and volunteer information for training related purposes and reporting to external agencies. • Collection of staff and volunteer health information as it relates to training purposes. • Project work involving stakeholder engagement.

Directorate	Functions	Primary dealings with personal and/or health information
	<u>Training Delivery</u> • Learning Management Systems • Training and Resources • Exercise Planning and Design • Training Advisors	
People and Development	People and Development set the strategic direction for the design, development and delivery of human resource and work, health and safety strategies, initiatives and programs that are aligned to SES operational and strategic requirements. People and Development comprises the following areas: <u>HR Services</u> • Member Services • Member Relations <u>Volunteer Strategy</u> • Volunteer Strategy • Volunteer Engagement <u>HR Advisory</u> • Member Relations • Talent Development • Diversity and Inclusion <u>Probity and Standards</u> • Professional Standards	• Human resource management, including the collection of sensitive personal information concerning staff members, volunteers and contractors. • Administration of personal information provided to the NSW SES as part of the volunteer membership application process (may include information obtained from criminal history checks, reportable conduct as defined under section 25(A) of the *Ombudsman Act 1974* (NSW) or child related work under section 6 of the *Child Protection (Working with Children) Act 2012* (NSW). With respect to these Acts, the NSW SES may provide information to the Police, Office of the Children's Guardian and/or the Ombudsman in accordance with agency responsibilities under these Acts. • Collection of staff members' health information insofar as the information does nor pertain to their continued suitability for appointment as a public section official* • Collection of volunteers' (and where relevant salaried members) health information, particularly information concerning their fitness to be recruited or to continue as members of the NSW SES, or as it relates to injuries incurred during NSW SES duties. • Investigations of grievances and disciplinary matters involving staff members and/or volunteers

Directorate	Functions	Primary dealings with personal and/or health information
	<u>Work, Health and Safety</u> • Safety, Health and Wellbeing • Peer Support • Chaplaincy • Injury Management	(particularly where the investigations involve the collection of evidence from internal and external witnesses). This may involve liaison with agencies such as Police, the Ombudsman or Children's Guardian. • Investigating serious allegations against staff and/or volunteers including serious misconduct or breaches of discipline, corruption, potential criminal and other high-risk matters (such investigations may involve the collection of evidence from internal and external witnesses). • Project work involving stakeholder engagement.
Information and Communications Technology	<u>Business Systems</u> • Cyber Security • Resource Systems <u>Operational Support</u> • Network Administration • IT Communications • Server Administration • Service Desk <u>Operational Systems</u> • Data Analytics • Records and Information • Systems Developer • Systems Architect	• ICT records, including records of external access to NSW SES websites. • Database entry, administration, extraction and storage (including Power BI). • Project work involving stakeholder engagement.

Directorate	Functions	Primary dealings with personal and/or health information
Finance, Asset and Business Services	<u>Finance</u> • Business Service Support • Accounting • Payroll <u>Procurement and Logistics</u> • Contracts and Procurement • Logistics <u>Facilities and Fleet</u> • Fleet Replacement Program • Fleet • Facilities	• Capture staff and volunteer details for vendor management and reimbursement purposes including personal details and bank accounts. • Capture of personal information relating to the issue of corporate credit cards. • Payroll administration and management, particularly in the collection of staff bank account details, tax file numbers, superannuation providers. • Drivers license details. • CCTV recordings from security cameras. • Collection of personal information through the Kiosk facility at reception, which used to sign people into the building. • Project work involving stakeholder engagement.
Org Strategy, Planning and Performance	<u>Enterprise PMO</u> • Business Analysis • Project Management Office • Change Managements <u>Governance and Policy</u> • Governance • Policy <u>Stay Safe Keep Operational</u> • SSKO Program	• Project work involving stakeholder engagement. • Collection of staff and volunteer information, for training related purposes (SSKO)

Directorate	Functions	Primary dealings with personal and/or health information
Other Corporate Services	<u>Office of the Commissioner</u> • Government Relations and Legal <u>Office of the Deputy Commissioner Operations</u> • Protocol and Special Events • Honours and Awards <u>Media and Communications</u> • Media and Public Relations • Digital Marketing • Internal Communications	• Ministerial correspondence and briefings, including briefings regarding sensitive and contentious matters related to NSW SES activities. • Dealing with access applications under the *Government Information (Public Access) Act 2009* (NSW). • Dealing with complaints and requests for internal review under the PPIPA and HRIPA. • Responding to subpoenas and orders to produce. • Information obtained for parliamentary inquiries, coronial inquests and litigation and other matters to which NSW SES is a party. • Administering Honours and Awards. • Community engagement and awareness activities
** This plan does not apply to information collected for the specific purpose of recruiting NSW SES staff members, or assessing suitability of NSW SES staff members continuing their appointment as public sector officials, recruitment or retention of paid NSW SES staff members. This is because section 4(3)(j) of the PPIPA stipulates that information concerning suitability of a 'public sector official' is not personal information within the context of the PPIPA.* *A public sector official is defined under the PPIPA as including a person employed or engaged by a public sector agency.*		

5 Implementation of the Information Protection Principles and Health Protection Principles

5.1 Collection

The NSW SES collects personal and health information for a number of reasons. Information is collected by the NSW SES so that it can discharge its functions under the SES Act, including to facilitate its engagement with members, to facilitate its internal business operations (including assessing membership applications and maintaining employment records), to correspond with members and for compliance with its legal obligations. The personal information relates to both staff and volunteer members of the SES as well as member of other agencies and the public it has dealings with.

Personal and health information is collected in a number of ways including:

- correspondence (written and electronic),
- forms (such as member application form),
- telephone and radio conversations,
- databases administered by the NSW SES (such as SAP and Beacon).
- CCTV footage,
- as part of its investigations.

Wherever possible, NSW SES will collect personal and health information directly from the individual to whom the information relates to unless collection from a third party has been authorised by the person. If a person is under 16 years of age, personal information will be collected from the person's parent or guardian.

The NSW SES provides a privacy notice when collecting personal and health information. Privacy notices contain information outlining the purpose for which the information is collected, how it will be used and disclosed and how it is stored.

The NSW SES will take reasonable steps to ensure that the personal and health information it collects is relevant, accurate, complete, up-to-date and not excessive. To assist with that determination, the NSW SES considers factors including the following:

- the purpose for which the information was collected,
- the sensitivity of the information,
- how many people will have access to the information,
- the importance of accuracy to the proposed use,
- the potential effects of the individual concerned if the information is inaccurate, out-of-date or irrelevant,
- the opportunities to subsequently correct the information,

- the ease which the information can be checked.

Unsolicited Information

The NSW SES will not have collected a person's personal or health information if the receipt of that information is unsolicited (that is, not asked for by the NSW SES). This is referred to in section 4(5) of the PPIPA.

However, the NSW SES will have 'solicited' information if it has a structure in place to receive the information and the information is relevant to a purpose of the agency. An example of this is the "Contact Us" page on the NSW SES website, where a person enters in their name and contact details. Another example is calls to the '132 500' number which is dedicated to those requesting assistance from the NSW SES.

5.2 Storage

The NSW SES ensures it has records management and storage policies in place that are consistent with the requirements of the *State Records Act 1998* (NSW). Reasonable security measures are maintained, including technical, physical and administrative actions, to protect information from unauthorised access and misuse.

Information is stored in a variety of ways, including in databases, cloud storage, by third parties and in various physical office locations.

The NSW SES has several mechanisms in place to safeguard and secure the personal information it holds. These measures include (but are not limited to):

- restricting access to all IT systems and databases to ensure that only authorised users with a clear business need can access them,
- use of strong passwords for computer access and a mandatory requirement that all staff change computer access passwords on a regular basis,
- print on demand (secured printing),
- implementing and maintaining strong security software access across all network components in arrangements for data transmission (including encryption and password protection where appropriate), backup and storage,
- maintaining logs and audit trails which are monitored and retained on a regular basis,
- providing staff with access to secure storage spaces near workstations to secure documents and devices,
- physically securing sensitive and confidential information in locked rooms,
- implementing and observing a clear desk policy,
- adopting best practice in electronic and paper records management and complying with our obligations under the *State Records Act 1998* (NSW),
- keeping information for only as long as necessary or as required by law,

- destroying information in a secure manner as appropriate (for example, using locked recycling bins and shredders),

- where it is necessary for information to be transferred to a third-party provider for the purposes of providing a service, contract terms are developed and executed to prevent unauthorised use or disclosure of information,

- providing information security awareness training to NSW SES members.

The official NSW SES records management system has a number of levels of access which limit access to personal or sensitive information. Information relating to criminal charges or convictions obtained by the NSW SES through the membership application process or through the course of investigations is stored securely by the People and Development Directorate. Access is limited to the relevant personnel and the records are held securely and disposed of in accordance with relevant record management legislation.

5.3 Access and Accuracy

The NSW SES takes reasonable steps to ensure the information it holds and uses is relevant, accurate, up-to-date and not misleading, having regard for the purposes for which it was collected and any purpose directly related to that purpose. The NSW SES has processes in place to enable staff and volunteers to access and update their personal and health information.

Individuals have a right to know:

- whether NSW SES holds their personal information;
- the nature of the personal information being held;
- the main purpose for which it is being used; and
- how they can access their information (and ensure valid requests for access proceed without excessive delay or expense).

NSW SES members (staff and volunteers)

Staff can access and update their personnel file by making a request to Member Relations (membership@ses.nsw.gov.au). Staff can also request Member Relations to update, correct or amend their personal or health information.

Volunteers are able to access their member file by making a request to their relevant Zone Headquarters or through Member Relations (membership@ses.nsw.gov.au). Volunteers are able to request an amendment to their member file by making a request to their relevant Zone Headquarters or through Member Relations.

Staff and volunteers can also change and update their basic personal information, such as contact details, via mySES and the SAP self-service portal.

Files about disciplinary matters and grievances are confidential. Access to personal information held on these files can be made by completing an application to "Access to Own Personal Records Application" form or using the contact details in Part 12.

Members of the public

A member of the public can access personal records held by NSW SES by completing an application to "Access to Own Personal Records Application" form or using the contact details in Part 12.

Access to information under the *Government Information (Public Access) Act 2009* (NSW) (GIPAA)

Anyone is able to seek access to their information that is held by the NSW SES under the GIPAA. Sometimes, the information that is requested includes personal and health information of other people. There are certain considerations that are taken into account before any information of this type is released. Further information about GIPPA is located on the NSW SES website.

5.4 Use

The NSW SES will only use personal and health information for the purpose which it was collected. The NSW SES will take reasonable steps to ensure that the personal information it collects is not used for an unlawful secondary purpose, and that it is accurate, up-to-date, and not misleading. That purpose is set out in the relevant privacy notice.

A directly related secondary purpose is a purpose that is very closely related to the purpose for collection and would be the type of purpose that people would quite reasonably expect their information to be used for.

Some examples of where the law permits the use personal or health information for another (secondary) purpose include:

- quality assurance activities such as monitoring, evaluating and auditing
- work health and safety laws require that we use information to ensure the safety of our employees
- unsatisfactory professional conduct or breach of discipline
- the information relates to a person's suitability for appointment or employment as a public sector official
- finding a missing person
- preventing a serious and imminent threat to life, public health and safety of a person.

Uses of personal and health information held by the NSW SES include:

- uses in connection with the preparation for and performance of emergency and rescue services;
- the assessment of a person's suitability for membership or continuity of membership in the NSW SES (including disciplinary and grievance investigations),
- the assessment of a member's suitability to undertake a training or development program,
- membership information used for operational and statistical purposes,
- analysis and reporting on diversity statistics,
- reporting of training engagements and outcomes to external bodies,
- research,
- to correspond with our members; and

- for compliance with NSW SES's legal obligations.

Staff and volunteer's understanding of their responsibilities concerning the appropriate use of personal and health information will be enhanced and kept up-to-date via appropriate privacy training and awareness programs.

5.5 Disclosure

The NSW SES will only disclose personal and health information for the purposes for which it is collected or if a secondary purpose is directly related to the primary purpose for which the information was collected, and the individual would reasonably expect the NSW SES to disclose that information for a secondary purpose. If NSW SES wants to disclose information for other purposes it will only do so with a person's consent (unless a relevant exemption applies) or in circumstances where to do so is permitted or required by law. The NSW SES can also disclose an individuals' personal and health information for a secondary purpose if it believes, on reasonable grounds, that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life, health or safety of a person or a serious threat to public health or safety.

Generally, prior to considering whether personal information may be disclosed (even where consent is available or it is lawful to do so), NSW SES will consider whether it is reasonable to do so by considering the following:

- the recipients of the information,
- the sensitivity of the information,
- the number of people who may access the information,
- the possible effects of disclosure on the individual concerned,
- the urgency with which the information is required (for example, an emergency situation may render the disclosure of personal information reasonable),
- the capacity to inform the person concerned, and obtain consent to the disclosure of their personal or health information,
- the seriousness and nature of any threat to life or health.

<u>Sensitive Information</u>

Disclosing sensitive information (eg your ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities) is only allowed with your consent or if there is a serious and imminent threat to a person's life or health.

NSW SES may need to collect sensitive personal and health information for:

- administration of its staff and volunteer membership,
- Nationally Co-ordinated Criminal History Record Checking process.

The NSW SES makes every effort to minimise the amount of information we collect about your ethnic or racial origin, political opinions, religious or philosophical briefs, trade union

membership or sexual activities. Where this information is collected, it is treated with the highest protection possible. The NSW SES will not disclose this information unless it is reasonably necessary for law enforcement purposes, is required by law or if the disclosure is necessary to prevent a serious or imminent threat to the life or health of a person. We may also disclose this information on an anonymised basis in connection with analysis and reporting on diversity statistics.

Disclosure outside NSW

Disclosing personal or health information to someone outside of NSW, or to a Commonwealth agency, is only permitted in limited circumstances as set out in the PPIPA or HRIPA.

Where information needs to be disclosed outside the NSW jurisdiction or to a Commonwealth agency, additional criteria must be met, including:

- that the recipient is subject to a privacy law that upholds principles for dealing with information in similar terms to the information protection principles,
- the individual concerned has consented,
- the transfer will benefit the individual concerned, but it is impracticable to obtain their consent, and if notified the individual would likely consent, or
- the disclosure is reasonably believed by the NSW SES to be necessary to lessen or prevent a serious and imminent threat to life, health or safety of the individual or another person.

5.6 Identifiers, anonymity and linkage of health records

The NSW SES may only assign identifiers to an individual's health information if it is reasonably necessary. The NSW SES must not include health information in a health records linkage system without a person's consent.

NSW SES has no linkages to any health records systems.

Wherever it is lawful and practicable, the NSW SES will give individuals the opportunity to remain anonymous. However, in the context of assessing member applications and during a member's engagement with the NSW SES, it is generally impracticable to interact with an individual anonymously due to the type of information required from an individual.

6 Exemptions

The PPIPA and HRIPA contain exemptions from compliance with certain IPPs and HPPs. The main exemptions to each principle are:

Limiting our collection of personal and health information – IPP 1 and HPP 1

- unsolicited information
- personal information collected before 1 July 2000
- health information collected before 1 September 2004
- in the case of personal information, for certain Ministerial correspondence
- in the case of personal information, to enable the auditing of accounts of performance of an agency or agencies
- in the case of personal information, certain research purposes

How we collect personal and health information – the source – IPP 2 and HPP 3

- unsolicited information
- personal information collected before 1 July 2000
- health information collected before 1 September 2004
- in the case of personal information, some law enforcement or some investigative and complaints handling purposes
- where another law authorises or requires us not to comply with this principle
- where non-compliance is otherwise permitted, implied or contemplated by another law
- in the case of personal information, where compliance would disadvantage the individual

Notification when collecting personal and health information – IPP 3 and HPP 4

- unsolicited information
- personal information collected before 1 July 2000
- health information collected before 1 September 2004
- the individual concerned has expressly consented to the non-compliance
- some law enforcement and investigative or complaints handling purposes
- where another law authorises us not to comply
- where non-compliance is otherwise permitted, implied or contemplated by another law
- where compliance would disadvantage the individual
- where notification about health information would be unreasonable or impracticable

How we collect personal and health information – the method and content - !PP 4 and HPP 2

- unsolicited information
- personal information collected before 1 July 2000
- health information collected before 1 September 2004
- law enforcement or some investigative and complaints handling purposes
- where another law authorises or requires us not to comply
- where non-compliance is otherwise permitted, implied or contemplated by another law
- where compliance would disadvantage the individual

Retention and Security – IPP 5 and HPP 5

- in the case of health information, the organisation is lawfully authorised or required not to comply
- in the case of health information, non-compliance is permitted under an Act or any other law

Transparency – IPP 6 and HPP 6

- if another law authorises or requires us not to comply
- where non-compliance is otherwise permitted, implied or contemplated by another law
- where the provisions of the GIPAA that impose conditions or limitations

Access - IPP 7 and HPP 7

- some health information collected before 1 September 2004
- where another law authorises or requires us not to comply
- where non-compliance is otherwise permitted, implied or contemplated by another law
- the provisions of the GIPAA that impose conditions or limitations

Correction – IPP 8 and HPP 8

- some health information collected before 1 September 2004
- some investigative or complaints handling purposes
- if another law authorises or requires us not to comply
- where non-compliance is otherwise permitted, implied or contemplated by another law
- the provisions of the GIPAA that impose conditions or limitations

Accuracy – IPP 9 and HPP 9

- there are no direct exemptions to the operation of this principle

Use – IPP 10 ad HPP 10

- the individual concerned has consented to the non-compliance
- law enforcement and some investigative or complaints handling purposes
- where another law authorises or requires us not to comply
- where non-compliance is other permitted, implied or contemplated by another law
- in the case of health information, to lessen or prevent a serious threat to public health or public safety
- the case of health information, compassionate reasons in limited circumstances
- finding a missing person
- information sent to other agencies under the administration of the same Minister or Premier for the purposes of informing the Minister or Premier
- in the case of health information, some research and training purposes

Identifiers – HPP 12

- there are no direct exemptions to this principle

Linkage of health records – HPP 15

- health information collected before 1 September 2004
- where another law authorises or requires us not to comply
- where non-compliance is otherwise permitted, implied or contemplated by another law

7 Public Registers

The NSW SES does not maintain any public registers for the purposes of the PPIPA or the HRIPA.

8 Your Review and Complaint Rights

If you have any concerns about the way your personal or health information has been handled, or you disagree with the outcome of your request to access or amend your personal or health information, you have the right to both an internal review of the decision by the NSW SES or external review by the Information and Privacy Commission (IPC) or the NSW Civil and Administrative Tribunal (NCAT), depending on the situation.

8.1 Direct Contact

If you have a complaint about the way your personal or health information has been handled, or disagree with the outcome of your application to access and/or amend your personal and health information, you are encouraged to discuss any concerns with the NSW SES Privacy Officer (see Part 12).

8.2 Internal review

General Principles

The following general principles are relevant to applications for internal review of privacy complaints:

- you may apply to NSW SES for an 'internal review' of the conduct you believe breaches the IPP or HPP, or you may make a privacy complaint directly to the NSW Privacy Commissioner
- complaints to the Privacy Commissioner can only result in a conciliated outcome, rather than a binding determination
- you cannot seek an internal review for an alleged/potential breach of someone else's privacy, unless you are an authorised representative of the other person
- an application for internal review must be made within six months from when you first became aware of the conduct you are concerned about (in limited circumstances we may consider a late application for internal review).

How to Apply for Internal Review

You have the right to ask for an internal review if you think your privacy has been breached.

An application for internal review must:

- be in writing
- be addressed to the NSW SES
- specify an address in Australia to which you can be notified after the completion of the review.

To apply for an internal review, you can submit the 'Internal Review (Privacy) Application' form or send your application and any relevant material by email or post at the details provided in Part 12.

You must lodge your request for internal review within six months from the time you first became aware of the conduct that you think breached your privacy.

Internal Review Process

The internal review will be conducted by a person who:

- was not involved in the conduct which is the subject of the complaint
- is a staff member of the NSW SES, and
- is qualified to deal with the subject matter of the complaint.

The NSW SES will acknowledge receipt of an internal review and will aim to:

- complete the internal review within 60 calendar days, and

- respond to you in writing within 14 calendar days of completing the internal review.

The internal review is conducted in accordance with the process set out in the Information & Privacy Commission's 'Internal Review Checklist'. When the internal review is completed, the applicant will be notified in writing of:

- the findings of the review
- the reasons for those findings
- the action we propose to take
- the reasons for the proposed action (or no action), and
- the applicant's entitlement to have the findings and the reasons for the findings reviewed by the NSW Civil and Administrative Tribunal.

A copy of your internal review request and the draft internal review report will be sent to Privacy Commissioner. Any submissions made by the Privacy Commissioner must be considered as part of the review. A final copy of the internal review decision will also be provided to the Privacy Commissioner.

If the internal review is not completed within 60 days or if you are dissatisfied with the NSW SES's findings, you have a right to seek a review of the conduct by the NCAT within 28 days of being notified of the internal review decision.

8.3 External Review

If you are unhappy with the outcome of the internal review, you can apply to NCAT to review the decision (an 'external review'). You may also apply to NCAT to conduct an external review if we have not completed your internal review within 60 days. Generally, you have 28 days from the date of our internal review decision to seek the external review.

NCAT has the power to make binding decisions on an external review, including ordering the payment of damages up to $40,000.

For more information about seeking an external review, including current forms and fees, please contact NCAT:

- Phone: 1300 006 228
- Address: Level 10, John Maddison Tower, 86-90 Goulburn Street, Sydney NSW 2000
- Website: www.ncat.nsw.gov.au

If you are not satisfied with the determination of the NCAT, you have a right to appeal to the Appeal Panel of the NCAT.

8.4 Complaint to Privacy Commissioner

You have the right to complain directly to the Privacy Commissioner about the NSW SES' conduct. However, the Privacy Commissioner may conduct a preliminary assessment of a complaint and decide not to deal with a complaint if satisfied that it would be more appropriate for you to request the NSW SES to conduct an internal review.

Complaints can be made to the Privacy Commissioner at:

- Mail: GPO Box 7011, Sydney NSW 2001
- Email: ipcinfo@ipc.nsw.gov.au

- Phone: 1800 472 679

9 Offences

It is a criminal offence, punishable by up to two years' imprisonment to:

- intentionally disclose or use personal or health information about another person to which you have access in doing your job, for any purpose other than that which is authorised
- offer to supply personal or health information that has been disclosed unlawfully
- hinder the Privacy Commissioner or a member of their staff from doing their job.

Part 8 of the PPIPA and the GRIPA provide further details about offences regarding personal and health information.

Section 308H of the *Crimes Act 1900* provides that it is an offence to access or modify restricted data held as computer records where authorisation has not been provided.

10 Other Related Laws

GIPAA and Government Information (Public Access) Regulation 2009 (NSW)

Under this law people can apply for access to government information we hold. Sometimes this information may include personal or health information. The GIPAA contains public interest considerations against disclosure of information that would reveal an individual's personal information or contravene an information protection principle or health privacy principle under PPIPA and HRIPA.

If a person has applied for access to someone else's personal or health information we will usually consult with the affected third parties. If we decide to release a third party's personal information despite their objections, we must not disclose the information until the third party has had the opportunity to seek a review of our decision.

When accessing government information of another NSW public sector agency in connection with a review, the Information Commissioner must not disclose this information if the agency claims that there is an overriding public interest against disclosure. For more information on the operation of the GIPAA and your personal information, please contact NSW SES GIPA (see Part 12 for the contact details).

Government Information (Information Commissioner) Act 2009 (GIIC Act) (NSW)

Under this law the Information Commissioner has the power to access government information held by other NSW public sector agencies for the purpose of conducting a review, investigation or dealing with a complaint under the GIPAA and GIIC Act. The Information Commissioner also has the right to enter and inspect any premises of a NSW public sector agency and inspect any record. This Act also allows the Information Commissioner to provide information to the NSW Ombudsman, the Director of Public Prosecutions, the Independent Commission Against Corruption or the Police Integrity Commission. For further information on the operation of the GIIC Act, contact the IPC (either on 1800 472 679 or by email, at ipcinfo@ipc.nsw.gov.au).

Privacy Act 1988 (Cth) (Privacy Act)

The NSW SES is not generally required to comply with the Australian Privacy Principles in the Privacy Act as it is not an 'organisation' within the meaning of the Privacy Act.

However, the NSW SES is a 'file number recipient' for the purposes of the Privacy Act because it holds records of employees which contain tax file number information. As such, the NSW SES must comply with any rules relating to tax file number information issued under s 17 of the Privacy Act. The NSW SES must ensure that any information provided by the NSW SES to another organisation is protected to the same standards that the NSW SES applies to the information it holds. The Privacy (Tax File Number) Rule 2015 (TFN Rule) only applies to the TFN information of individuals and does not apply to TFN information about other legal entities such as corporations, partnerships, superannuation funds and trusts. The TFN Rule is legally binding. A breach of the TFN Rule is an interference with privacy under the Privacy Act. Individuals who consider that their TFN information has been mishandled may make a complaint to the Office of the Australian Information Commissioner (OAIC).

Data Sharing (Government Sector) Act 2015 (NSW)

Under this law the sharing of government data between government agencies and the government Data Analytics Centre is regulated. This includes the sharing of de-identified personal data. Enhanced privacy safeguards apply and the usage of personal and health information must be in line with current privacy legislation.

Crimes Act 1900 (Cth)

Under this law there are offences regarding accessing or interfering with data in computers or other electronic devices.

Independent Commission Against Corruption Act 1988 (NSW)

Under this law, information cannot be misused if the information was obtained in the course of someone doing their job for the NSW SES.

Public Interest Disclosures Act 1994 (NSW) (PID Act)

The PID Act sets in place a system to encourage public officials to report wrongdoings. The NSW SES is responsible for receiving complaints made as public interest disclosures under the PID Act.

The definition of personal information under the PPIP Act excludes information contained in a public interest disclosure. This means that 'personal information' received or collected under the PID Act is not subject to the IPPs or HPPs.

The PID Act requires the NSW SES to not disclose information that might identify or tend to identify a person who has made a public interest disclosure.

State Records Act 1998 (NSW) *and State Records Regulation 2015* (NSW)

The NSW SES is required to comply with this legislation. Under this law, the management and destruction of records is regulated and overall guidance is provided on the practical requirements for effective records and information management including retention periods and disposal of records.

11 Reviewing and Promoting this Plan

11.1 Reviewing the Plan

This Plan will be reviewed at a minimum every two years, but more frequently when legislative, administrative or systemic changes occur that affect the way we manage the personal information and health information we hold.

11.2 Promoting the Plan

Public awareness

This plan will be made publicly available as open access information under the GIPAA. We aim to promote public awareness of this plan by:

- publishing the plan on our website in a format that is accessible to the widest possible audience
- providing copies of the plan free of charge on request
- telling people about the plan when we answer questions about how we manage personal information and health information

NSW SES Executive

The NSW SES executive team is committed to transparency about how we comply with the PPIPA and HRIPA, which is reinforced by:

- endorsing the plan and making it publicly available
- reporting on privacy in our annual report in line with the *Annual Reports (Departments) Act 1985* (NSW) and *Annual Reports (Departments) Regulation 2015*
- using the plan as part of induction

NSW SES Members

The NSW SES will ensure its members are aware of this plan and how it applies to the work they do by:

- writing this plan in a practical way so that members can understand what their privacy obligations are, how to manage personal and health information and what to do if unsure about their privacy obligations
- publishing this plan on the intranet
- providing members with access to training so they understand their privacy obligations and how they are to manage personal and health information
- highlighting the plan at least once a year (for example, during Privacy Awareness Week)

12 Contacts

12.1 NSW SES Privacy Officer

For further information about this plan, the personal and health information we hold, or if you have any questions or concerns, please contact the NSW SES Manager, Government Relations and Legal, who is the NSW SES Privacy Officer and GIPA contact:

- Mail: PO Box 6126, Wollongong NSW 2500
- Email: gipa@ses.nsw.gov.au
- Phone: (02) 4251 6129
- Web: www.ses.nsw.gov.au

Document Control Sheet

Title	*Privacy Management Plan*
Current Version #	2.0
Key Email Contact	gipa@ses.nsw.gov.au
Directorate	Office of the Commissioner
Policy Owner	Manager, Government Relations and Legal
Policy Sponsor	Chief of Staff
Effective date	05 December 2022
Next Review Date	05 December 2024
Rescinds	Privacy Management Plan (21 Feb 2018)
Topic	Compliance
Function	Governance
Key Words	Privacy, health personal information, health information

Approval

Title	Version	Date
Manager, Government Relations and Legal	2.0	25 November 2022
Chief of Staff	2.0	25 November 2022
Commissioner	2.0	2 December 2022