Privacy Management Plan

Legal and Regulatory Services

Document ID: CG03-009
Issued: 17 November 2021

Key points:

Fire and Rescue NSW recognises that protecting privacy is essential to maintain the confidentiality of information and to protect the privacy rights of individuals.

Under the *Privacy and Personal Information Protection Act 1998* (the PPIP Act) all agencies must have adequate measures in place to ensure they protect privacy. FRNSW has developed this Privacy Management Plan to support the PPIP Act.

Who should read this document?

Everyone in FRNSW needs to understand privacy management; however, this Plan is targeted at staff with a role in information management and usage and will be involved in the collection, use, disclosure and storage of information.

Implementation and monitoring

This document is part of FRNSW's management of privacy risks and is supported by information management policies and procedures, which document privacy strategies. The Legal and Regulatory Services branch reviews this document every two years.

Contents

1 Overview

1.1 Purpose

This Privacy Management Plan (Plan) explains how FRNSW manages personal information in line with the *Privacy and Personal Information Protection Act 1998 (NSW)* (the PPIP Act) and health information in accordance with the *Health Records and Information Privacy Act 2002 (NSW)* (the HRIP Act).

We have a Privacy Management Plan to manage and protect the personal information FRNSW manages. The Plan also explains how to contact FRNSW about the personal and health information it holds, how information can be accessed and amended and how privacy complaints are handled.

The Plan aims to:

- meet the requirement for FRNSW to have such a plan under s 33 of the PPIP Act
- demonstrate to members of the public how we meet our obligations under the PPIP Act and the HRIP Act
- provide staff with the necessary knowledge and skills to manage personal and health information appropriately and in accordance with the law
- enhance the transparency of our operations, and
- illustrate our commitment to respecting the privacy rights of customers, clients, staff and members of the public.

This Plan uses plain language to describe our legal obligations and how FRNSW will comply with them. We have chosen to simplify the language in order to make our obligations easier to understand.

1.2 What this Plan covers

Section 33(2) of the PPIP Act sets out the requirements of this Plan. This Plan must include:

- information about FRNSW's policies and practices to ensure compliance with the PPIP Act and the HRIP Act
- how staff are made aware of these policies and practices
- the internal review procedures, and
- anything else considered relevant to the Plan in relation to privacy and the roll out of the protective notice for personal and health information that FRNSW holds.

1.3 When this plan will be reviewed

This Plan will be reviewed regularly to determine if there are any legislative or administrative changes that affect the management of personal and health information by FRNSW. This Plan will be updated every two years, or earlier if the need arises.

2 Introduction

2.1 About FRNSW

FRNSW is the State Government agency responsible for the provision of prevention and education, fire, rescue and hazmat services in cities and towns across New South Wales in

accordance with *the Fire and Rescue NSW Act 1989,* the *State Emergency and Rescue Management Act 1989* and other related legislation.

FRNSW is one of the world's largest urban fire and rescue services. Its purpose is to enhance community safety, quality of life and confidence by minimising the impact of hazards and emergency incidents on the people, property, environment and economy of NSW. FRNSW is one of the key agencies involved in responding to emergency and disaster events throughout NSW. More detailed information is available on FRNSW's website.

2.2 Privacy context at FRNSW

FRNSW is a 'public sector agency' for the purposes of the PPIP Act and the HRIP Act, by virtue of the definitions of 'public sector agency' provided in s 3(1) of the PPIP Act and s 4(1) of the HRIP Act. Staff collect, hold, use and disclose personal and health information for the purpose of carrying out FRNSW's functions.

The PPIP Act and the HRIP Act set out privacy principles that FRNSW must comply with. The PPIP Act covers personal information other than health information and includes 12 Information Protection Principles (IPPs). The IPPs cover the information life cycle from collection to disposal. The IPPs include obligations with respect to data security, data quality and rights of access and amendment to personal information, as well as how personal information may be collected, used and disclosed.

Health information is regulated by a different set of principles set out in the HRIP Act. Health information is a type of personal information about the physical or mental health of an individual or information provided or generated in the delivery of a health service. There are 15 Health Privacy Principles (HPPs). Like the IPPs, the HPPs cover the information life cycle but include additional principles with respect to anonymity, trans-border data flows, linkage of health records and the use of unique identifiers.

There are exemptions to many of the privacy principles. Exemptions can be found in the PPIP Act and the HRIP Act, and in regulations, privacy codes of practice and public interest directions. Where exemptions are particularly relevant to FRNSW, they have been noted in Section 4 of this Plan.

2.3 Privacy management at FRNSW

All staff are responsible for complying with privacy legislation. Advice and support are available from the Privacy Contact Officer for day-to-day privacy matters. This centralised model provides strategic management across the organisation for training, education, advisory and compliance services and coordination of forms, templates and other material provided to the public. It provides a single-entry point for customers seeking privacy-related services or information.

2.4 Privacy Contact Officer

The Privacy Contact Officer acts as the focal point in FRNSW for all matters related to privacy and the handling of personal and health information.

The role of the Privacy Contact Officer is to:

- provide advice to management, staff and business partners on privacy and the application of the PPIP Act and the HRIP Act
- provide a first point of contact for members of the public for matters related to privacy and the handling of personal and health information
- train and educate staff in aspects of the PPIP Act and the HRIP Act
- conduct internal reviews into possible breaches of the PPIP Act and the HRIP Act, except where it is appropriate for another person to undertake the review
- ensure any privacy-related policies and procedures are up-to-date and are published, and
- develop privacy-related educational materials for staff and members of the public.

The Privacy Contact Officer can be contacted as follows:

Post:
Privacy Contact Officer
Legal and Regulatory Services
Fire and Rescue NSW
Locked Mail Bag 12 Greenacre NSW 2190

Phone: 02 9269 6451
Email: PrivacyOfficer@fire.nsw.gov.au

2.5 Responsibilities of staff

Management must ensure that their staff are aware of their privacy responsibilities and any associated privacy policies, procedures, guidelines and standards, including this Plan.

All staff are required to comply with the PPIP Act and the HRIP Act, including the IPPs and HPPs when handling personal and health information held by FRNSW. Both Acts contain criminal offence provisions applicable to public sector officials and persons who misuse personal and health information; see Section 4 of this Plan for more details.

Staff should identify whether any of their new projects, policies, or programs are likely to raise any privacy issues. The NSW Information and Privacy Commission has developed a checklist to assist staff to identify when they should consult their agency's Privacy Contact Officer. Staff should complete the checklist and contact the Privacy Contact Officer if necessary.

All Directors are required to review the personal information held by their divisions on a regular basis to ensure they comply with the FRNSW Privacy Policy and this Plan.

This Plan aims to help staff to understand and comply with their obligations under both the PPIP Act and the HRIP Act. If staff are uncertain as to whether certain conduct may breach their privacy obligations, they should seek advice from the Privacy Contact Officer.

3 Personal and health information held by FRNSW

3.1 What is personal information?

Personal information is defined in s 4 of the PPIP Act. In summary, personal information is information or an opinion about an individual whose identity is apparent or could be reasonably determined. Common examples of personal information include a person's name, bank account details, fingerprints, a photograph or video. It includes information that is recorded (e.g. on paper or contained in a database) and also information that is not recorded (e.g. verbal conversations). A person's identity may be apparent where neither the name nor a photograph is involved, but the information about the person is such that their identity could be inferred.

Exclusions as to what constitutes personal information can be found at *ss 4(3)* and *4A of the PPIP Act*. There are 13 exclusions to the definition of personal information under the PPIP Act. Some of these exclusions include:

- information about an individual who has been dead for more than 30 years
- information about an individual that is contained in a publicly available publication, and
- information about an individual's suitability for employment as a public sector official

Common examples of information falling within the exclusions include recruitment records, referee reports and performance appraisals, and information that is published or available on the internet. The PPIP Act also excludes certain information that may be held in connection with some activities authorised under different legislation.

For more information on these exclusions refer to ss 4(3) and 4A of the PPIP Act or contact the Privacy Contact Officer.

3.2 What is health information?

Health information is defined in s 6 of the HRIP Act. Health information means:

- personal information that is also information or an opinion about:
  - a person's physical or mental health or disability
  - a health service provided, or to be provided, to a person
  - a person's wishes about the future provision of health services to themselves
- other personal information collected to provide a health service
- other personal information about an individual collected in connection with the donation of an individual's body parts, organs or body substances, or
- genetic information that is or could be predictive of the health of a person or their relatives or descendants.

Exclusions as to what constitutes health information pursuant to the HRIP Act can be found at s 5(3) of the HRIP Act. There are 15 exclusions to the definition of health information under the HRIP Act, which include the exclusions listed above. An example of information

excluded by the HRIP Act is the results of a pre-employment medical check to assess a person's suitability for a job at FRNSW.

For more information on these exclusions, refer to s 5 of the HRIP Act or contact the Privacy Contact Officer.

3.3 Main kinds of personal and health information held by FRNSW

FRNSW has a range of functions requiring or involving the collection of personal information, including:

- providing prevention and education, fire, rescue and hazmat services
- consultation with the community, businesses and other stakeholders
- recording, investigating, and managing complaints and allegations
- incident management and reporting
- compliance with industrial awards
- enforcing regulations and legislation
- employing staff and engaging volunteers, and
- provision of health and safety support services FRNSW employees.

Personal information may be collected by FRNSW in any of the following ways:

- personnel records
- incident reports
- application forms
- financial transaction records
- contracts
- compensable and non-compensable return to work
- superannuation management, and
- records of health and safety support services.

Personal information may be collected electronically, in writing, over the telephone or radio and in person.

FRNSW holds a range of personal and health information in several locations and in a range of formats. The main kinds of personal and health information held by FRNSW and a brief explanation of how those kinds of information are related to FRNSW's functions and activities are set out below:

- personal information from persons volunteering to participate in Safety Visits for the purposes of policy, planning and the improvement of fire safety services.
- personal information relating to community consultation participants, such as regional forums, including details of survey responses for the purposes of research and policy development.
- personal information for the purposes of contracting service providers.
- personal and health information related to audit and risk works, including audit evidence collected during the performance of approved audit projects.

- personal information collected through engagement with customers (including the broader community) to gather insights that help inform the development of policy and strategy to drive service delivery improvements.
- personal and health information about individuals involved in incidents for the purposes of improving reporting, research and planning in support of safety strategies and policies.
- incident records including audio recordings, images and CCTV footage for fire, rescue and hazmat incidents for the purpose of improving response, safety and community outcomes and to assist insurance recovery, law enforcement and investigative agencies.
- infringements and sanctions data to respond to traffic infringements and inform road safety policies and strategies.
- personnel records for staff, including medical certificates and other information related to fitness for work, timesheets, grade and salary range and other personnel records that contain private information.
- return to work information includes medical certification, independent and treating medical reports and clinical notes relating to a specific injury
- superannuation management includes all relevant medical certification and reports, including clinical notes relating to all injuries regarding capacity for work.
- records of health and safety support services including vaccination records.

4 How FRNSW manages personal and health information

There are 12 Information Protection Principles (IPPs) and 15 Health Privacy Principles (HPPs) that FRNSW must comply with when handling personal and health information. These are summarised together below.

4.1 Collection – IPP1 to 4 and HPP1 to 4

FRNSW will only collect personal and health information if it is for a lawful purpose that is directly related to one of our functions and it is reasonably necessary for us to have the information.

FRNSW collects personal or health information directly from the person unless the person has authorised otherwise or, in the case of health information, it would be impractical for the person to do so. FRNSW may collect personal or health information from a third party where it is provided for within the PPIP Act or the HRIP Act, or under other legislation.

When collecting personal or health information about an individual, FRNSW will take reasonable steps to notify the person that we are collecting that information and the purposes for which the information is being collected. Where reasonably practicable FRNSW provides written notification to individuals that their personal information is being collected, and where this is not practicable FRNSW notifies individuals through advice on its website.

When collecting information from an individual, FRNSW will:

- not collect excessive personal or health information
- not collect personal or health information in an unreasonably intrusive manner, and

- ensure that personal and health information collected is relevant, accurate, up-to-date and complete by providing templates and procedures for specific information collection.

4.2 Storage – IPP5 and HPP5

FRNSW will take reasonable security safeguards to protect personal and health information from loss, unauthorised access, use, modification or disclosure, and against all other misuse. We will ensure personal and health information is stored securely, not kept longer than necessary, and disposed of appropriately.

FRNSW has policies and procedures on the security of personal and health information, including storage, access and disposal that follow legislative requirements.

4.3 Access and accuracy – IPP6 to 9 and HPP6 to 9

FRNSW will enable anyone to know, on request to the Privacy Contact Officer:

- whether FRNSW is likely to hold their personal and health information
- the nature of the personal and health information
- the main purposes for which FRNSW uses their personal and health information, and
- their entitlement to access their personal and health information.

FRNSW will allow people to access their personal and health information without excessive delay or expense. Access will only be refused where authorised by law. We will allow people to update or amend their personal and health information, to ensure it is accurate, relevant, up-to-date, and complete (see section 6).

Before using personal or health information, FRNSW will take reasonable steps to ensure that the information is relevant, accurate, up-to-date, and complete.

4.4 Use – IPP10 and HPP10

FRNSW may use personal and health information for:

- the primary purpose for which it was collected
- a directly related secondary purpose
- another purpose where it is reasonably necessary to prevent or lessen a serious and imminent threat to life or health, or
- another purpose for which the person has consented.

4.5 Disclosure – IPP11 to 12 and HPP11 to 15

FRNSW may disclose personal and health information if:

- the disclosure is directly related to the purpose for which the information was collected, and FRNSW has no reason to believe that the individual concerned would object to the disclosure
- the individual is reasonably likely to be aware, or has been made aware, that this kind of information is usually disclosed to the recipient, and
- the disclosure is reasonably necessary to prevent or lessen a serious and imminent threat to life or health.

FRNSW will not disclose sensitive personal information relating to an individual's racial, ethnic information, political, religious and philosophical beliefs, sexual activity and trade union membership unless the person has consented to the disclosure or when it is necessary to prevent a serious and imminent threat to life or health.

In terms of health information, FRNSW:

- will only identify individuals by using unique identifiers if it is reasonably necessary for us to carry out our functions
- does not currently use a health records linkage system, and
- does not usually transfer health information outside NSW.

Where is it is lawful and practicable, FRNSW will give the option to provide services anonymously.

4.6 Exemptions

Exemptions to the IPPs and HPPs are discussed in a general way below. Different exemptions may apply between an IPP and its equivalent HPP. If in doubt, the wording of the exemptions contained within the PPIP Act and the HRIP Act should be consulted, and guidance sought from the Privacy Contact Officer or Privacy Commissioner.

The exemptions include:

- unsolicited information if it contains personal information
- personal information used for law enforcement or investigative purposes
- some information exchanges with other NSW public sector agencies, and
- personal information used for the purposes of some types of research.

The *Commonwealth Telecommunications Act 1997* also provides some exemptions as part of a triple zero emergency call processes.

FRNSW may not be required to comply with some principles if lawfully authorised or required not to do so, or to lessen or prevent a serious threat to public health or safety.

4.7 Public interest directions

Under section 41 of the PPIP Act, the Privacy Commissioner, with the approval of the Attorney General, may make Public Interest Directions to waive or modify the requirement for a public sector agency to comply with an IPP. For further information on public interest directions currently in operation please refer to the Information and Privacy Commission.

4.8 Memoranda of understanding

FRNSW has several Memoranda of Understanding (MOU) and other agreements with various bodies for access to personal information. These MOUs provide a degree of assurance that information is accessed, stored, maintained and disclosed for an agreed purpose within the terms of the MOU or agreement.

Several relevant MOUs are published on FRNSW's intranet and website and in the agency's Annual Report, while further details about relevant MOUs are available from the Privacy Contact Officer.

4.9 Privacy codes of practice

The PPIP Act and the HRIP Act permit the development of privacy codes of practice by an agency that may modify the application of an IPP, HPP or public register provision. At the time of this Plan's publication, a privacy code of practice or health privacy code of practice has not been developed by FRNSW.

4.10 Public registers

Part 6 of the PPIP Act prescribes special rules for personal and health information held on public registers. These rules regulate when personal or health information contained in a public register can be disclosed. FRNSW does not maintain any public registers for the purposes of the PPIP Act or the HRIP Act.

4.11 Offences

Both the PPIP Act and the HRIP Act contain criminal offence provisions applicable to public sector officials and persons who misuse personal and health information.

The table below summarises these offences.

Offence	Maximum penalty	Legislative provision
It is a criminal offence for a public sector official to corruptly disclose and use personal or health information.	Fine of up to 100 penalty units ($11,000) or imprisonment for two years, or both.	s 62 the PPIP Act s 68 the HRIP Act
It is a criminal offence for a person to offer to supply personal or health information that has been disclosed unlawfully.	Fine of up to 100 penalty units ($11,000) or imprisonment for two years, or both.	s 63 of the PPIP Act and s 69 of the HRIP Act.
It is a criminal offence for a person – by threat, intimidation or misrepresentation – to persuade or attempt to persuade an individual: • to refrain from making or pursuing a request to access health information, a complaint to the Privacy Commissioner or the NSW Civil and Administrative Tribunal, or an application for an internal review; or • to withdraw such a request, complaint or application.	Fine of up to 100 penalty units ($11,000).	s 70(1) of the HRIP Act.
A person must not – by threat, intimidation or misrepresentation – require another person to give consent under the HRIP Act, or require a person to do, without consent, an act for which consent is required.	Fine of up to 100 penalty units ($11,000).	s 70(2) of the HRIP Act.

Offence	Maximum penalty	Legislative provision
It is a criminal offence for a person to: • wilfully obstruct, hinder or resist the Privacy Commissioner or a member of the staff of the Privacy Commissioner • refuse or wilfully fail to comply with any lawful requirement of the Privacy Commissioner or a member of the staff of the Privacy Commissioner, or • wilfully make any false statement to or mislead, or attempt to mislead, the Privacy Commissioner or a member of the staff of the Privacy Commissioner in the exercise of their functions under the PPIP Act or any other Act.	Fine of up to 10 penalty units ($1,100).	s 68(1) of the PPIP Act

5 Management of Data Breaches

5.1 Data Breach Notification Schemes

5.1.1 The Notifiable Data Breaches (NDB) Scheme

The NBD Scheme was established by the passage of the *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Clth) and came into effect on 22 February 2018. It is aimed primarily at federal government and private sector agencies. However, FRNSW has obligations under the NDB Scheme regarding data breaches that relate to Tax File Numbers (TFNs).

If it is an eligible data breach, along with general management of the breach, FRNSW is required to notify affected individuals and the Office of the Australian Information Commissioner (OAIC). The notification will include recommendations about the steps individuals should take in response to the breach. There are exceptions to notifying in certain circumstances.

5.1.2 Sharing of Government Sector Data

The *Data Sharing (Government Sector) Act 2015* (NSW) (DSGS Act) has a data breach notification scheme in respect of sharing of government sector data under the DSGS Act with the NSW Data Analytics Centre, or between other government sector agencies.

If FRNSW receives personal or health information from another agency and becomes aware that privacy legislation has been (or is likely to have been) breached, FRNSW is required to inform the data provider and the NSW Privacy Commissioner (IPC) of the breach as per the DSGS Act.

5.1.3 European Union's General Data Protection (GDPR) Regulation

The *General Data Protection Regulation* (GDPR) applies from 25 May 2018 to any organisation offering goods or services to, or monitoring the behaviour of, individuals living in the European Union (EU).

The GDPR does not usually apply to services provided by FRNSW, however, if in extenuating circumstances a data breach required reporting under this regulation FRNSW is required to notify the lead EU supervisory authority within 72 hours and to notify the affected individuals without undue delay if required.

FRNSW will provide information on GDPR responsibilities prior to deployment in relevant destinations.

5.1.4 NSW Privacy Commissioner's Voluntary Reporting Scheme

NSW does not currently have a mandatory notifiable data breach reporting requirement however the Privacy Commissioner has a voluntary reporting scheme in place. The voluntary scheme encourages agencies that have experienced a serious data breach to report the details of the breach to the Privacy Commissioner, so that the Privacy Commissioner can assess the breach, provide advice or investigate.

5.2 Reporting data breaches

In accordance with the Information Security Policy a data breach or allegation of a data breach must be notified immediately to the relevant line manager, the IT Service Desk or the Chief Information Security Officer (CISO), A data breach includes where IT equipment

(FRNSW issued phones, laptops, FRNSW database, USBs etc.) has been compromised or lost.

Where data breaches or allegations of data breaches include personal or health information about individuals, the Privacy Contact Officer should also be notified.

5.3 Data Breach Response Plan

If a data breach or allegation of a data breach is reported, FRNSW will take step to:

5.3.1 Contain the breach

This may include searching for and recovering the data, confirming that no copies were made or that the information was destroyed by the party receiving it, conducting a remote wipe on a lost portable device, implementing a computer system shut down, or changing passwords and system user names.

5.3.2 Evaluate and Mitigate the Risks

Remedial action will be taken to minimise the likelihood that the breach will result in harm to any individual. For example, depending on the type of data breach, employees might be told to change passwords, not to open emails with attachments, and to be aware of phishing attacks. An assessment of the likely harm resulting from a data breach will be conducted as soon as practicable.

5.3.3 Notify and Communicate

If it is determined that the data breach requires notification under one of the data breach notification schemes the relevant parties will be informed. FRNSW will notify the NSW Privacy Commissioner of a data breach where required and when the circumstances indicate that it is appropriate to do so.

5.3.4 Prevent Future Breaches

FRNSW will investigate the cause of the breach and consider developing a prevention plan to mitigate the risk of any future data breaches.

6 Privacy and other legislation relating to personal and health information

6.1 Privacy legislation

- *Privacy and Personal Information Protection Act 1998* (NSW)
- *Health Records and Information Privacy Act 2002* (NSW)
- *Privacy and Personal Information Protection Regulation 2014* (NSW)
- *Health Records and Information Privacy Regulation 2017* (NSW)
- Privacy Codes of Practice, Directions and Statutory Guidelines made under the PPIP Act and the HRIP Act

6.2 Other relevant legislation and policy

Other legislation that may also affect the application of the privacy principles includes, but is not limited to:

- *Criminal Records Act 1991* (NSW)
- *FRNSW Privacy Policy*
- *Government Information (Public Access) Act 2009* (NSW)
- *Independent Commission Against Corruption Act* (NSW)
- *NSW Cyber Security Policy*
- *Ombudsman Act 1974* (NSW)
- *Public Interest Disclosures Act 1994* (NSW)
- *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Clth)
- *State Records Act 1998* (NSW)
- *Surveillance Devices Act 2007* (NSW)
- *Workplace Surveillance Act 2005* (NSW)
- *Telecommunications Act 1997* (Clth)
- *Telecommunications (Interception and Access) Act 1979* (Clth)

7 How to access and amend personal and health information held by FRNSW

7.1 Request to access and amend

People wishing to access or amend personal and health information FRNSW holds about them should contact the member of staff or unit holding the information.

The request should:

- include name and contact details
- state whether the application is made under the PPIP Act (personal information) or the HRIP Act (health information)
- explain what personal or health information is to be accessed or amended
- explain how the personal or health information is to be accessed or amended.

7.2 Limits on accessing or amending information

FRNSW is prohibited from providing access to another person's personal and health information. However:

- under section 26 of the PPIP Act, a person can give FRNSW consent to disclose their personal information to someone that would not normally have access to it
- under sections 7 and 8 of the HRIP Act, an "authorised person" can act on behalf of someone else, and
- FRNSW may be authorised to disclose health information, such as in the event of a serious and imminent threat to the life, health and safety, to find a missing person or for compassionate reasons.

8 Privacy complaints and reviews

A person who wishes to make a complaint or request a review in relation to privacy may:

- resolve the matter informally
- apply for an internal review by FRNSW, or
- contact the Privacy Commissioner.

Complaints related to breaches of privacy with regards to:

- personal information collected before 1 July 2000, and
- health information collected before 1 September 2004

will be managed under FRNSW's general complaints process as the PPIP Act and the HRIP Act do not apply to personal information collected before those respective dates.

8.1 Resolving the matter informally

FRNSW encourages people to try to resolve privacy concerns with FRNSW informally, or at least contact the Privacy Contact Officer to discuss the issue, before lodging an application for internal review.

8.2 Internal review

Individuals have the right to seek an internal review under Part 5 of the PPIP Act if they think that FRNSW has breached the PPIP Act or the HRIP Act relating to their own personal and health information. Individuals cannot seek an internal review for a breach of someone else's privacy, unless they are authorised representatives of the other person.

8.2.1 Internal review process

Applications for an internal review must:

- be made within six months from when the applicant first became aware of the matter
- be made in writing
- have an address within Australia to which a notice can be sent, and
- be addressed to the FRNSW Privacy Contact Officer.

FRNSW will:

- acknowledge receipt of an internal review as soon as possible
- notify the Privacy Commissioner of the request for internal review, and
- complete an internal review as soon as is reasonably practicable in the circumstances.

The Privacy Contact Officer will usually conduct the internal review unless it is appropriate for another person to be appointed to do so. FRNSW will inform the applicant of the progress of the internal review and will respond in writing within 14 calendar days of determining the internal review.

The Privacy Commissioner is entitled to make submissions to FRNSW regarding internal reviews. Where the matter is in relation to health information, the Privacy Commissioner may undertake the internal review.

8.2.2 External review by the NSW Civil and Administrative Tribunal

An applicant may seek an external review by the NSW Civil and Administrative Tribunal (NCAT) if the internal review is not completed within 60 days or if the applicant is unhappy with the results of the internal review. NCAT will assess whether or not the agency complied with its privacy obligations.

The time frames in which NCAT applications are permitted for review of a privacy matter are:

1. If the internal review was completed within 60 days, then the time frame for applicants seeking to make an application is **28 calendar** days after the day on which the applicant was notified of the result of the internal review.

2. If the internal review **was not** completed within 60 days, then the time frame for applicants seeking to make an application is **28 calendar days** after the **later** date of either:
   a) when the applicant was notified of the result of the internal review, or
   b) the day on which the 60 day period expires.

Contact details for the NSW Civil and Administrative Tribunal are:
Phone: 1300 006 228

8.3 Privacy Commissioner

Privacy complaints may also be made directly to the Privacy Commissioner. Complaints directed to the Privacy Commissioner can only result in conciliated outcomes.

Contact details for the Information and Privacy Commission are:
Email: ipcinfo@ipc.nsw.gov.au
Phone: 1800 472 679

9 Promoting privacy

FRNSW reinforces compliance with the PPIP Act and the HRIP Act by:

- endorsing this Plan and making it publicly available
- providing a copy of this Plan to relevant oversight bodies such as the FRNSW Audit and Risk Committee
- reporting on internal reviews to the Information and Privacy Commission, and
- identifying privacy issues when implementing new systems, services and processes.

FRNSW promotes awareness of privacy obligations among staff by:

- publishing this Plan and FRNSW's privacy-related policies on FRNSW's intranet and website
- publishing information about privacy on FRNSW's intranet
- communicating regularly with staff about privacy
- ensuring contractors engaged by FRNSW are aware of their privacy obligations
- ensuring FRNSW policies comply with privacy legislation

- including the Plan in induction packs, and
- providing training and advice to staff.

9.1 Public awareness

This Plan provides information to members of the public about how FRNSW manages personal and health information. The Plan is publicly available as open access information under the GIPA Act.

FRNSW promotes public awareness of FRNSW's Privacy Management Plan by:

- publishing the Plan on FRNSW's website
- providing hard copies of the Plan free of charge on request
- translating the Plan into other languages on request, and
- informing people about the Plan when responding to enquiries about personal and health information.

10 Annexure A

10.1 Privacy Protection Notice

Under section 10 of the *Privacy and Personal Information Protection Act 1998 (NSW)* (the PPIP Act), when FRNSW collects personal information from an individual, such as their name, address, telephone number or email address, FRNSW must make the individual aware of:

- the purposes for which the information is being collected
- the intended recipients of the information
- whether the supply of the information is required by law or is voluntary
- any consequences for the individual if the information (or any part of it) is not provided
- ways the individual can access and correct the information, and
- the name and address of the unit that is collecting the information and the unit that is to hold the information.

FRNSW's Privacy Protection Notice appears below:

PRIVACY PROTECTION NOTICE

Purpose of collection: *state the purposes for which the information is being collected*

Intended recipients: *to whom (including business units or organisations) the information will be disclosed*

Supply: *whether the supply of the information is required by law or is voluntary and any consequences for the individual if the information (or any part of it) is not provided*

Access/ Correction: *how the individual can access and correct the information*

Storage: *the name and address of the business unit that is collecting the information and the business unit that is storing the information.*

The Privacy Protection Notice will be introduced and progressively included on requests for personal information from individuals.

A sample privacy protection notice for the home visits program is available on the intranet.

Procedure Manager	Manager Legal and Regulatory Services
Contact Officer	Privacy Contact Officer
Contact No	92696451
Document type	Procedure
Applies to	☑ Firefighters ☑ Community Fire Unit Members ☑ Administrative and Trades Staff ☑ Contractors and Consultants
Status	Approved
Security	Unclassified
File Reference	NFB/00389
Review Date	1 December 2023
Rescinds	V3 Privacy Management Plan
Copyright	© State of New South Wales through Fire and Rescue NSW