NSW GOVERNMENT

NSW RURAL FIRE SERVICE

PRIVACY MANAGEMENT PLAN

LEGAL AND GOVERNMENT INFORMATION

21 December 2018

Document control

Release history

Version	Date	Author	Summary of changes
1.0	4 August 2014	Manager, Secretariat Audit and Legal	-
1.1	21 December 2018	Director Executive Services	Updates to Directorate information and how directorates may deal with a person's personal or health information. Inclusion of Health Privacy Principles. Advice on when personal or health information is taken to be 'held' by the NSW RFS. Inclusion of exemptions of 'investigation' and 'information exchange' as specific exemptions under the PPIPA. New Parts 9 (Privacy Reviews) and 10 (Notifiable Data Breaches) added.

Reviewed by

Name	Title	Date
Debbie Andreatta	Director Executive Services	19/12/18

Approved by

Name	Title	Date
Stephen O'Malley	Executive Director Finance and Executive Services	20/12/18
Shane Fitzsimmons AFSM	Commissioner	24/12/18

Related documents

Document name	Version
Service Standard 1.1.14 Personal Information and Privacy	2.5
Service Standard 1.1.3 Grievances	3.1
Service Standard 1.1.9 Child Related activities	4.0
Service Standard 1.1.26 Volunteer and Visitor Access to Network Services & Data	1.1
Service Standard 1.1.30 Public Interest Disclosures	2.0
Service Standard 1.4.3 Public Access to Government Information	1.0
Service Standard 1.4.5 Social Media	2.0

Service Standard 1.4.6 Websites	2.1
Service Standard 1.4.8 Media	1.0
Service Standard 2.1.3 Brigade Registers	2.1
Service Standard 2.1.6 Joining the NSW RFS as a Volunteer Member	3.2
Service Standard 6.1.3 Training in the NSW RFS	4.1
P5.1.6 Records Management	3.0
P6.1.4 Bush Fire Hazard Complaints and notices and associated Guidelines	1.0
NSW RFS Corporate Governance Statement	Dec 2017

Contents

Introduction 1

1 Legislation 1

1.1 The Privacy and Personal Information Protection Act 1998 (PPIPA) 1

1.2 The Health Records and Information Protection Act 2002 (HRIPA) 4

2 The functions and structure of the NSW RFS 6

3 Dealing with personal information 7

4 Implementation of the Information Protection Principles 13

4.1 Collection 13

4.2 Retention and Security 14

4.3 Access and alteration 15

4.4 Use 16

4.5 Disclosure 16

5 Exemptions and privacy codes of practice 17

5.1 The Government Information (Public Access) Act 2009 17

5.2 Specific exemptions from principles 17

5.3 Public interest directions 18

5.4 Privacy Codes of Practice 18

6 Public Registers 18

7 Policies and Procedures 18

8 Raising awareness of privacy obligations 19

8.1 Annual communiqué relating to privacy 20

8.2 Privacy training and awareness 20

8.3 Review of forms 20

9 Privacy complaints and reviews 20

9.1 Your right to internal review 20

9.2 Your right to external review 22

10 Notifiable data breaches 23

10.1 Tax File Number Collection 23

10.2 Sharing Government Sector data 23

11 Offences 23

12 Reviewing this Plan 24

13 Appendix A – Implementation Plan 25

Introduction

The NSW Rural Fire Service (NSW RFS) recognises that privacy is an issue of concern for its members as well as members of the public. In New South Wales, the *Privacy and Personal Information Protection Act 1998* (PPIPA) outlines a series of mandatory standards that public sector agencies are required to comply with when handling personal information.

Section 33 of PPIPA requires government agencies to develop and implement a Privacy Management Plan.

This Plan has been prepared to comply with that requirement and articulates the responsibilities of the NSW RFS under both the PPIPA and the *Health Records and Information Privacy Act 2002* (HRIPA).

A Privacy Management Plan is an important resource in ensuring that all NSW RFS staff and volunteers are aware of the agency's and their responsibilities and obligations with respect to personal information and can deal with this information in a responsible, transparent and effective way. It informs members of the public about how the NSW RFS collects, manages and handles the personal and health information it holds.

The Plan outlines:

a. The legislation that underpins the way in which the NSW RFS deals with personal information;

b. The kinds of personal information and health information as defined in PPIPA and HRIPA that the NSW RFS holds;

c. The NSW RFS' Service Standards, policies and procedures to ensure compliance with the principles of the PPIPA and HRIPA;

d. The manner in which these policies are distributed to NSW RFS staff/volunteers;

e. The NSW RFS' procedures for conducting internal reviews for alleged breaches of privacy.

1 Legislation

1.1 The Privacy and Personal Information Protection Act 1998 (PPIPA)

The PPIPA provides a framework for the handling of personal information by government agencies and resolving complaints concerning the handling of this information. While the PPIPA recognises a person's right to privacy that right is not absolute. Accordingly, the Act provides for a number of exemptions and exceptions to privacy principles.

In doing so, the PPIPA works to strike a balance between a person's right to privacy and the rights of an agency to effectively perform its functions.

Personal Information

PPIPA regulates the way that public sector agencies deal with 'personal information' to protect a person's privacy.

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 recorded in material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion'.*

What does personal information include?

Personal information includes such things as a person's:

- name

- address
- family life
- financial information
- fingerprints and photos
- body samples or genetic characteristics.

Information that meets the definition is not limited to a person's private or personal affairs. The definition is not confined to information contained in written format. An opinion, from which a person's identity can reasonably be ascertained, can also constitute personal information of a person even if it is not recorded.

What is not personal information?

Section 4(3) of the PPIPA outlines some exceptions to the definition of 'personal information'. Exceptions relevant to the NSW RFS include:

- Information about a person who has been dead for more than 30 years;
- Information contained in a publicly available publication;
- Information about a person contained in a public interest disclosure under the *Public Interest Disclosures Act 1994;*
- Information about a person arising out of an authorised operation under the *Law Enforcement (Controlled Operations) Act 1997*;
- Information about a person arising out of a Royal Commission or Special Commission of Inquiry;
- Information about a person contained in Cabinet or Executive Council documents under the *Government Information (Public Access) Act 2009*;
- Information or an opinion about a person's suitability for employment as a public sector official.

When is personal information 'held' by the NSW RFS?

Personal information is held by the NSW RFS 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 RFS 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.*

The Information Protection Principles under PPIPA

Sections 8-19 of PPIPA set out the 12 Information Protection Principles (IPPs) which establish the acceptable way in which agencies may deal with personal information.

The IPPs outlines the obligations placed on public sector agencies, including the NSW RFS, with respect to personal information. The IPPs provide guidance as to how personal information should be secured, the circumstances where it should be amended, as well as how personal information may be collected, used and disclosed.

Collection

- **IPP 1 -** Personal information may only be collected for purposes which are lawful and which directly relate to the functions or activity of the agency; and the collection of that information is reasonably necessary for that purpose.
- **IPP 2 -** Personal information must be collected directly from the individual to whom the information relates, unless the individual has authorised the collection of the information from someone else.
- **IPP 3 –** The individual to whom the personal information relates must be aware that his/her information is being collected, the purposes for which the information is being collected and the intended recipients of the information.

  The principle also requires agencies to tell the person how they can view and correct their personal information, and any consequences that may apply if they decide not to provide their information to an agency.
- **IPP 4 –** Agencies must take reasonable steps to ensure that the information it collects is relevant, accurate, up to date and complete, and that the collection of the information does not intrude to an unreasonable extent on the personal affairs of the person.

Retention and security of personal information

- **IPP 5 –** Information stored by an agency must be kept no longer than necessary. Agencies must ensure that personal information is disposed of securely and in accordance with any requirements for the retention and disposal of personal information.

  The principle also requires agencies to ensure that information is protected by reasonable security measures and that it is protected from unauthorised use or disclosure when it has been made available to any third party providing a service to the agency.

Access and accuracy

- **IPP 6 –** Individuals are entitled to ascertain whether an agency holds personal information and to access information about the nature and purpose of the personal information held, and their entitlement to gain access to the information.
- **IPP 7 –** Agencies that hold personal information must, at the request of the individual to whom the information relates and without excessive delay or expense, provide the individual with access to the information.
- **IPP 8 –** Agencies which hold personal information must, at the request of the individual to whom the information relates, make appropriate amendments to ensure that the personal information is accurate, relevant, up to date, complete and not misleading.

Use

- **IPP 9 –** Public sector agencies are obliged to take reasonable steps before using personal information to ensure that the information is accurate, relevant, up-to-date, complete and not misleading.
- **IPP 10 –** Personal information should only be used for the purpose that it was collected, for a purpose that is directly related to the purpose for collection, for a purpose that the individual has consented to or where the use is necessary to prevent or lessen a serious or imminent threat to the life or health of any person.

Disclosure

- **IPP 11 –** Personal information should only be disclosed with a person's consent, or if they were told at the time that it would be disclosed. The disclosure must be directly related to the purpose for which it was collected, and there is no reason to believe that the person would object. A person's personal information may also be disclosed if disclosure is necessary to prevent a serious or imminent threat, to any person's health or safety.
- **IPP 12 –** Personal information of a particularly sensitive nature (such as information about an individual's racial or ethnic origin, political opinions, religious beliefs, health or sexual orientation) must not be disclosed unless the disclosure is necessary to prevent a serious or imminent threat to the life or health of any person.

1.2 The Health Records and Information Protection Act 2002 (HRIPA)

Health information is a particular type of personal information. Section 6 of HRIPA defines **'**health information' as personal information that is information or an opinion about:

a) a person's physical or mental health or disability; or

b) a person's express wishes about the future provision of health services for themselves; or

c) a health service provided, or to be provided to a person; or

d) other personal information collected in relation to the provision of a health service.

Personal information about an individual collected in connection with organ donation, and personal information that is genetic information about an individual arising from a health service provided to that individual is also captured within the definition.

HRIPA stipulates the responsibilities of private organisations and public agencies in dealing with health information. It 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.

When is health information 'held' by the NSW RFS?

Health information is held by the NSW RFS 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 RFS 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.*

The Health Privacy Principles under HRIPA

Schedule 1 of HRIPA contains 15 Health Privacy Principles (HPPs) outlining how health information must be collected, held, used, disclosed and secured. The HPPs also provide for amendment and disposal of health information, and anonymity in the provision of health services.

The NSW RFS is committed to ensuring that all of its members discharge their responsibilities under HRIPA. The privacy compliance strategies at Part 5 have been developed to encourage compliance with not only PPIPA but also HRIPA.

Collection

- **HPP 1 –** Health information may only be collected for a lawful purpose that is directly related to a function or activity of an agency, and the collection of that information is reasonably necessary

for that purpose

- **HPP 2 –** Agencies that collect health information from a person must take such steps that are reasonable in the circumstances to ensure that the information collected is relevant to that purpose, is not excessive and is accurate, up to date and complete, and that the collection does not unreasonably intrude into the personal affairs of a person.
- **HPP 3 –** An agency must collect health information about a person only from that person, unless it is' unreasonable' or 'impracticable' to do so. Health information is to be collected in accordance with any guidelines issued by the Privacy Commissioner.
- **HPP 4 –** Agencies must, at or before the time that it collects health information, inform the person as to why it is collecting health information, what will be done with it, and who else may see it. Agencies must also tell the person how they can view and correct their health information, and any consequences that will occur if they decide not to provide their information to them.

  If an agency collects health information about a person from a third party it must still take reasonable steps to notify the person that this has occurred.

Retention and security of health information

- **HPP 5 –** An agency that holds health information must ensure that:
  - the information is kept for no longer than is necessary for the purposes for which the information may lawfully be used, and
  - the information is disposed of securely and in accordance with any requirements for the retention and disposal of health information, and
  - the information is protected by taking such security safeguards as are reasonable in the circumstances, against loss, unauthorised access, use, modification or disclosure, and against all other misuse, and
  - if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or disclosure.

Access and accuracy

- **HPP 6 –** Agencies must explain to a person what health information is being stored, the reason it is being used and any rights they have to access the health information.
- **HPP 7 –** Agencies that hold health information must, at the request of the person to whom the information relates, and without excessive delay or expense, provide the individual with access to the information.
- **HPP 8 –** Agencies must, at the request of the person to whom the health information relates, make appropriate amendments to ensure that the person's health information is accurate, relevant, up to date, complete and not misleading.
- **HPP 9 –** Agencies must ensure that health information it holds is relevant, accurate, up to date, complete and not misleading before using it.

Use

- **HPP 10 –** Agencies should only use health information for the purpose for which it was collected, unless the person to whom the information relates has consented to their information being used for a secondary purpose.

Disclosure

- **HPP 11 –** Agencies must only disclose information for the purpose for which it was collected, or for a directly related purpose that a person would expect. In other cases, consent would be required.

Identifiers and anonymity

- **HPP 12 –** An agency can only identify people by using unique identifiers if it is reasonably necessary to carry out the agency's functions efficiently.
- **HPP 13 –** Wherever it is lawful and practicable, individuals must be given the opportunity to not identify themselves when entering into a transaction with, or receive health services from, an agency.

Transferrals and linkage

- **HPP 14 –** Agencies can only transfer health information outside NSW in accordance with Schedule 1, Clause 14 of the HRIP Act.
- **HPP 15 –** Agencies can only use health records linkage with the person's express consent as outlined in Schedule 1, Clause 15(2) of the HRIP Act.

2 The functions and structure of the NSW RFS

Section 3 of the *Rural Fires Act 1997* outlines the key objectives of the NSW RFS. These include the prevention, mitigation and suppression of bush fires, the co-ordination of bush fire fighting and bush fire prevention throughout the state, and the protection of people from injury or death, and property damage arising from fires. These objectives are supported by functions set out under section 9 of the *Rural Fires Act 1997.*

The NSW RFS is comprised of the NSW RFS Commissioner, salaried staff and volunteer rural fire fighters. The NSW RFS has over 72,000 volunteers, and is one of the largest and best trained fire services in the world.

While coordinated bush fire fighting, prevention and mitigation are its primary functions, the NSW RFS is also involved in critical community safety activities. These include:

- Providing advisory services relating to fire fighting
- Attending house and other structural fires
- Carrying out rescue operations allocated by the State Rescue Board
- Conducting community education programs
- Assisting the State Emergency Operations Controller in carrying out emergency management functions identified under the *State Emergency and Rescue Management Act 1989*
- Assisting agencies in dealing with any incident or emergency under the State Emergency Plan ('EMPLAN')
- Issuing bush fire warnings to community members at risk
- Identifying and designating Neighbourhood Safer Places throughout NSW
- Providing the AIDER (Assist Infirm, Disabled and Elderly Residents) program, a free one-off support program to vulnerable members of the community, to reduce their bush fire risk.
- Reviewing and approving development applications

Volunteer fire fighters of the NSW RFS fulfil a firefighting, prevention and protection role. State Mitigation Support Services support NSW RFS Brigades and districts across the State through hazard reduction works and the AIDER program.

Salaried staff are employed to manage the day-to-day operations of the Service at Headquarters, regional offices and district fire control centres.

The NSW RFS comprises the following Directorates:

- Operations
- Infrastructure Services
- Membership and Strategic Services
- Finance and Executive Services

3 Dealing with personal information

Each of the NSW RFS 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 RFS Directorates – Functions and dealings with personal and/or health information

Directorate	Functions	Primary dealing s with personal information
Operations	The Operations Directorate is responsible for undertaking the NSW RFS responsibilities relating to the prevention and response to bush fires. The Directorate coordinates the NSW RFS response to fires, mitigating the risk of fire through hazard reduction programs and engaging with the local community to be prepared. Operations encompasses the following units: <u>Community Resilience</u> • Development Planning and Policy • Environment and Hazard Services • Grant & Co-ordination Programs • Planning and Predictive Services <u>Co-ordinated Risk Management</u> • Major Projects <u>Response and Co-ordination</u> • State Operations • Aviation • Operational Doctrine and Standards • Emergency Management Co-ordination • Operational Business and Procurement <u>Operational and Mitigation Services</u> • State Mitigation Services • Operational Resources and Transport • Operational Mitigation Services Business Unit	• Receiving and responding to hazard complaints pursuant to part 4 of the Rural Fires Act 1997. • Issuing penalty notices in relation to prescribed offences pursuant to section 131 of the Rural Fires Act 1997. • Fire investigations, particularly those investigations involving witnesses and/or taking place on private property. This includes liaison with the NSW Police Force and other relevant agencies. • Responding to fire incidents. • Providing advice in relation to development applications. • Assessing development applications and planning. • Receiving requests for assistance through the Assistance for Infirm, Disabled and Elderly Residents Program (AIDER) • Audio recording information from callers to the Bush Fire Information Line (BFIL) • Recording of calls across the business at a state and local level in line with legislative requirements. • Providing advice to other agencies • Arson Trend Analysis System • Issuing fire permits • Applying for search warrants to investigate the cause and origin of fires. • Volunteer management, including (but not limited to)

Directorate	Functions	Primary dealing s with personal information
	• Remote Area Firefighting and Specialised Operations <u>Planning and Environment Services</u> • Planning and Environment • Development assessment and planning • Community protection planning <u>Regional Services</u> • Regions North, South, East and West • Regional Management. • Strategic Fire Trails	collection, retention and use of records of volunteers' personal information. This includes information contained in Brigade Registers. • Investigations of grievances and disciplinary matters (particularly where the investigations involve the collection of evidence from internal and external witnesses).
Finance and Executive Services	The Finance and Executive Services Directorate provides key corporate and executive support functions in the administration of the NSW RFS. The Directorate encompasses the following Units: <u>Finance and Program Management</u> • Financial Accounting • Management Accounting <u>Executive Services</u> • Legal and Government Information • Records • Committees and Projects <u>Corporate Communications</u> • Corporate and International Relations • Community Engagement • Organisational Communications	• Project work involving stakeholder engagement. • Ministerial correspondence and briefings, including briefings regarding sensitive or contentious matters related to the NSW RFS's activities. • Dealing with requests for information under the *Government Information (Public Access) Act 2009.* • Dealing with requests for internal review under the *Privacy and Personal Information Protection Act 1998.* • Responding to subpoenas and orders to produce. • Community engagement and awareness activities, including the recording of attendees at public meetings, records of members of interested community groups. • Information obtained for Coronial Inquests, Inquiries and litigation to which the NSW RFS is a party. • Capture all staff details for vendor management and reimbursement purposes including personal details and

Directorate	Functions	Primary dealing s with personal information
	• Media Services	bank accounts. • Capture of personal information relating to the issue of corporate credit cards.
Membership and Strategic Services	The Membership and Strategic Services Directorate comprises the following units: <u>Membership Services</u> • Health Safety and Welfare • Membership Administration • Membership Services <u>Corporate Planning, Risk and Learning</u> • Planning, Risk and Policy • Learning and Development • Library Services <u>Professional Standards</u> • Investigations <u>Volunteer Relations and Workforce Planning</u>	• Human resource management, including the collection of sensitive personal information concerning staff members and volunteers, including volunteers of the Volunteer Rescue Association. • Payroll administration and management, particularly in the collection of staff bank account details, tax file numbers, superannuation providers. • Administration of personal information provided to the NSW RFS as part of the volunteer membership application process (may include information obtained from nationally coordinated criminal history checks, reportable conduct as defined under section 25(A) of the *Ombudsman Act 1974* or child related work under section 6 of the *Child Protection (Working with Children) Act 2012.* With respect to these Acts, the NSW RFS may provide personal information to the Ombudsman, Police and/or the Office of the Children's Guardian in accordance with agency responsibilities under these Acts. • Collection of staff members' health information insofar as this information does not pertain to their continued suitability for appointment as a public sector official (see s. 4(3)(j))* • Collection of volunteers' (and where relevant salaried members) health information, particularly information

Directorate	Functions	Primary dealing s with personal information
		concerning their fitness to be recruited or to continue as volunteer members of the NSW RFS, or as it relates to injuries incurred in the course of their volunteer duties. • Investigations of grievances and disciplinary matters involving staff members (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 the 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). • 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 (such as medical information for Breathing Apparatus training). • Collection of staff and volunteers information as it relates to Awards (both Internal and External). • Collection of staff, volunteer, members of agencies and general public information as it relates to library membership. • Collection of information as part of conducting research, in line with the agreed ethical guidelines.

Directorate	Functions	Primary dealing s with personal information
Infrastructure Services	The Infrastructure Services Directorate leads the planning, approval, acquisition, construction, maintenance and disposal of the NSW RFS' infrastructure. The Directorate comprises the following Units: <u>Assets & Infrastructure</u> • Procurement • Fixed Assets and Infrastructure • Communication Systems <u>Engineering Services</u> • Safety Design Technology • Engineering Inspectorate <u>Information & Communications Technology</u> • Enterprise Architecture • ICT Applications and Development • ICT Business • ICT Programs • ICT Infrastructure and Operations	• Database entry, administration, extraction and storage. • ICT records, including records of external access to NSW RFS websites. • CCTV recordings from security cameras. • Drivers license details.

* This Plan does not apply to information collected for the specific purpose of recruiting NSW RFS staff members, or assessing the suitability of NSW RFS staff members continuing their appointment as public sector officials, recruitment or retention of paid NSW RFS staff members. This is because s4(3)(j) of the Act stipulates that information concerning suitability of a "public sector official" is not personal Information within the context of the Act.

A public sector official is defined under the Act as including a person employed or engaged by a public sector agency (s3 of the PPIP Act).

4 Implementation of the Information Protection Principles

4.1 Collection

The NSW RFS collects personal information for a wide variety of reasons. Broadly, this information is collected by the NSW RFS in order to discharge its functions under the *Rural Fires Act 1997*, and relates to the NSW RFS' volunteer and salaried members as well as members of other agencies and the public it has dealings with.

Personal information is collected through the following channels:

- The receipt of mail and electronic communications;
- Forms (such as volunteer application forms);
- Databases administered by the NSW RFS such as SAP;
- Telephone and radio conversations;
- As part of its investigations.

The NSW RFS has in place a number of practices and procedures to ensure compliance with the relevant Information Protection Principles when personal information is collected.

The NSW RFS always strives to collect information directly from the individual to whom it relates. However, it is not possible to do this in every case and occasionally the NSW RFS is required to collect information from an intermediary. Where practicable, the NSW RFS ensures that information collected from third parties is with the permission of the individual concerned.

The NSW RFS Service Standard *1.1.14 - Personal Information and Privacy* advises staff to obtain a signed authority or other proof where an individual is purporting to act on another's behalf (clause 3.2(b) of the Service Standard).

With respect to training data, the NSW RFS manages this data in line with National Vocational Education and Training Policy, which includes minimum mandatory content for inclusion in a Privacy Notice and Student Declaration.

Unsolicited information

The NSW RFS will not have collected a person's personal information if the receipt of that information is unsolicited (that is, the NSW RFS did not ask for it): section 4(5) of the PPIP Act.

However, the NSW RFS 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 NSW RFS' feedback form on its 'report a cigarette butt tosser' (www.rfs.nsw.gov.au/fire-information/cigarette-form) and 'reporting a bush fire hazard' (www.rfs.nsw.gov.au/plan-and-prepare/know-your-risk/Bush-fire-hazards-and-your-property/reporting-a-bush-fire-hazard) web pages.

The NSW RFS website also has a number of online forms that members of the public can complete to access various NSW RFS services as well as provide feedback. This includes requests for assistance through the AIDER program.

In the latter case, the provisions of the *Rural Fires Act 1997* (section 74C) requires a complainant to provide identifying information. The NSW RFS regularly reviews its application forms to ensure compliance with IPP 3 and the other 'collection' IPPs.

Sensitive information

The most detailed and sensitive personal information collected by the NSW RFS is in connection with the administration of its volunteer membership. The NSW RFS volunteer membership application form outlines the:

- reasons for the information collection
- how the information is used, and
- who will have access to the information.

The form also requires the applicant's acknowledgment and/or consent that s/he understands how the NSW RFS will handle the personal information provided and why it will be handled in this way.

With regard to sensitive information such nationally coordinated criminal history checks undertaken as a part of the application process, further explanatory material is available to applicants in the form of a guide outlining information relating to the Nationally Co-ordinated Criminal History Record Checking process.

The NSW RFS website also contains a privacy statement outlining what personal information is collected, how that information is used, the exceptions which apply and where personal information will be stored.

The privacy statement also informs individuals of their rights to request access to information stored about them, and makes it clear that the NSW RFS will not keep any personal information for longer than is necessary for the purposes for which it is used, and that information will be stored and disposed of securely. Further information can be found at www.rfs.nsw.gov.au/about-us/privacy.

Section 25 of the PPIPA provides that the NSW RFS is not required to comply with collection principles where another Act or law permits non-compliance. Some of the circumstances where non-compliance may be permitted are:

- When the NSW RFS is determining applications under the *Government Information (Public Access) Act 2009*;
- When the NSW RFS is discharging some of its functions under the *Rural Fires Act 1997.*

A particular example where it is critical that the NSW RFS is able to receive information from members of the public concerning third parties is when receiving bush fire hazard complaints. The NSW RFS must collect this information so that it can respond to and investigate complaints, issue notices and undertake hazard reduction works pursuant to Part 4 of the *Rural Fires Act 1997.*

Section 26 of the PPIPA also provides that the NSW RFS is not required to comply with collection principles if compliance would, in the circumstances, prejudice the interest of the individual to whom the information relates.

4.2 Retention and Security

The Records Unit is responsible for devising and implementing records management and storage policies consistent with the requirements of the *State Records Act 1998*. To that purpose the NSW RFS has in place a number of tools to safeguard and secure the personal information that it holds. These measures include (but are not limited to):

- Password protected systems, firewalls and anti-hacking software to protect NSW RFS information technology systems from unlawful intrusion;
- Internal policies and Service Standards, which provide staff and volunteers with guidance and direction as to the appropriate storage and security of records (including records which involve

personal information);

- Code of Conduct and Ethics which includes a section on Corporate and Personal Information; and
- Physical security systems, including electronic barriers to entry into the NSW RFS building and additional electronic and physical barriers to entry into the records storage area located at Headquarters.

The official NSW RFS records management system has a number of levels of access which limit access to personal information. The NSW RFS also has specific policies in place to ensure the security of sensitive personal information, such as personal information relating to grievances or information regarding criminal charges or convictions.

Information pertaining to criminal charges or convictions obtained by the NSW RFS through the membership application process or through the course of investigations is stored securely by the Membership Services section and/or the Professional Standards Unit. Access is limited to relevant personnel and the records are held securely and disposed of in accordance with relevant record management legislation.

The NSW RFS at times engages external consultants to conduct investigations. The NSW RFS also regularly reviews its information technology and physical security systems to ensure that information remains protected.

4.3 Access and alteration

The NSW RFS has existing processes in place to enable volunteers and staff to access and update their personal information. These requests are ordinarily made to the Membership and Strategic Services Directorate, and are dealt with by staff who are familiar with the provisions of PPIPA relating to access and amendment of personal information.

Members can also change and update their basic personal information, such as contact details, via MyRFS and the SAP employee self-service portal.

PIPPA only allows an individual to access their own personal information as defined under the Act. Access to health information should be made under the HRIPA provisions.

Both staff and members of the public may also request access to their personal information (and health information) in accordance with the provisions of the *Government Information (Public Access) Act 2009* (GIPA Act).

Where the information sought consists of a combination of the applicant's personal information and personal information of third parties or other non-personal information, an applicant may be advised that they need to submit a formal application under the GIPA Act provisions. This allows for third party consultation and review rights ensuring the privacy considerations of all parties can be taken into account prior to a decision being made regarding access.

Information that cannot be obtained under the GIPA Act cannot otherwise be obtained under PIPPA.

Complex requests for access to information are referred to the Manager, Legal and Government Information (LGI), who is the NSW RFS' designated Right to Information and Privacy Officer. The Manager, LGI makes a determination as to whether a request should be dealt with under PIPPA or HRIPA, or informally or formally under the GIPA Act.

Formal applications may be required where the information sought is overly time consuming or may involve third party information requiring consultation.

4.4 Use

NSW RFS staff and volunteers 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.

Uses of personal information held by the NSW RFS may include:

- Membership information used for brigade operational and statistical purposes;
- The assessment of a member's suitability to undertake a training or developmental program;
- The assessment of a member's suitability for membership or continuity of membership in the NSW RFS (including disciplinary and grievance investigations);
- Analysis and reporting diversity statistics;
- Issuing of notices pursuant to provisions under Part 4 (relating to bushfire hazard reduction complaints) and Part 7 (issuing penalty notices in relation to prescribed offences) of the Rural Fires Act 1997.
- Investigations including fire investigations and investigations into a bush fire hazard complaint
- Assessments as part of an application for a bush fire hazard reduction certificate
- Reporting of training engagements and outcomes to external bodies
- Research

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

4.5 Disclosure

The NSW RFS seeks to ensure that personal information is disclosed only with the permission of the individual concerned (where it is possible to obtain such permission), or where it is otherwise lawful to do so.

The IPPs and HPPs relevant to disclosure (Section 18 of PIPPA and HPP 11), do not prohibit the disclosure of personal information. Rather, it imposes limitations, with disclosure allowed under specified circumstances.

There are exemptions in both PIPPA and HRIPA of particular relevance to the NSW RFS which affect the application of the disclosure principles (refer section 5 below for further information).

Generally, prior to considering whether personal information may be disclosed (even where consent is available or it is lawful to do so), NSW RFS staff and volunteers will consider whether it is reasonable to do so in light of:

- 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 urgently necessary);

- The capacity to inform the individual concerned, and obtain consent to the disclosure of their personal or health information; or
- The seriousness and nature of any threat to life or health.

5 Exemptions and privacy codes of practice

PIPPA and HRIPA provide a number of exemptions to the operations of the principles contained in these Acts. Further, the Privacy Commissioner of NSW may make public interest directions or privacy codes of practice, which exempt an agency from complying with one or more personal information or health privacy principles, and modify the application of these principles respectively. Outlined below are two examples of exemptions of particular relevance to the NSW RFS.

5.1 The Government Information (Public Access) Act 2009

Section 5 of PIPPA and section 22 of HRIPA specifically provide that provisions in these Acts do not affect the operation of the GIPA Act. As such disclosure of personal or health information, pursuant to provisions of the GIPA Act, will not contravene the disclosure provisions in PIPPA and HRIPA.

Where an application for access to information involves third party personal or health information, the NSW RFS requires the applicant to submit a formal access application under the GIPA Act. This allows the NSW RFS, when reasonably practicable, to consult with the third parties in question prior to making a decision regarding release of such information.

Where an applicant or a third party seeks external review in relation to a NSW RFS decision with respect to a formal access application, the NSW RFS may disclose personal information contained in the GIPA file to the Information and Privacy Commission or the NSW Civil and Administrative Tribunal.

5.2 Specific exemptions from principles

Law enforcement purposes

The *Rural Fires Act 1997* authorises holders of certain positions in the NSW RFS to enter land to investigate the cause and origin of fire. Fire investigation is a shared responsibility between the NSW RFS and other agencies. The NSW RFS has an Interagency Fire Investigation Protocol with the NSW Police Force and Fire and Rescue NSW, which covers exchanges of information.

The NSW RFS also has a Memorandum of Understanding with the NSW Police Force in relation to information sharing pertaining to investigations in NSW.

A number of exemptions in PIPPA and HRIPA are of particular relevance to the NSW RFS in connection with this function. Section 23 of the PPIPA contains a number of exemptions specific to law enforcement agencies or public sector agencies in cases where the information being dealt with is for law enforcement purposes. Section 23(6A) allows personal information to be shared between public sector agencies where the collection, use or disclosure of that information is 'reasonably necessary for law enforcement purposes'.

Schedule 1 Clause 11(1)(j) of HRIPA enables health information to be disclosed where disclosure is reasonably necessary for the exercise of law enforcement functions.

Investigations

Section 24 exempts investigative agencies (e.g. the Ombudsman's Office and the Independent Commission against Corruption) from a number of privacy principles in certain circumstances. Section 24(6) extends these exemptions to situations where a public sector agency such as the NSW RFS is 'investigating or otherwise handling' a complaint which could be referred to, or made to, an investigative

agency, or that has been referred from an investigative agency to the RFS for investigation.

Information exchange

Section 27A of the PPIPA contains exemptions facilitating information exchanges between agencies that are reasonable necessary to enable agencies to deal with, or respond to correspondence from a Minister or Member of Parliament, inquiries to be referred to between agencies, or the auditing of accounts or the performance of agencies. Section 28(3) of the PPIPA also allows for information exchanges between agencies under the administration of the same Minister or the Premier in certain circumstances.

5.3 Public interest directions

There are currently no public interest directions in place for the NSW RFS.

5.4 Privacy Codes of Practice

PPIPA and HRIPA allow the development of privacy codes of practice by an agency. Privacy Codes of Practice may modify the application of an IPP or a HPP. No privacy codes of practice or health privacy codes of practice have been developed by the NSW RFS at the time of publication.

6 Public Registers

The NSW RFS does not currently administer any public registers.

7 Policies and Procedures

Policies and Service Standards are issued by the Commissioner under Section 13 of the *Rural Fires Act 1997*. The NSW RFS has a systematic framework in place for the development and review of new and existing Policies and Service Standards to ensure:

- the co-ordination of activities across NSW;
- regulatory compliance obligations are met;
- levels of service and tasks are undertaken in a consistent manner;
- facilitation of continuous improvement practices.

The Executive Director Membership and Strategic Services oversees this framework and the Policy Review Committee provides the governance for NSW RFS policy documents.

The NSW RFS has developed and implemented Service Standard *1.1.14 Personal Information and Privacy*, which deals with policies for compliance with privacy legislation. Service Standard 1.1.14 is also linked to a number of other key Service Standards which integrate privacy policy into key activities across the organisation and which ensure staff and volunteer compliance with privacy legislation. These policies include:

- Service Standard 1.1.3 Grievances
- Service Standard 1.1.7 Code of Conduct and Ethics
- Service Standard 1.1.9 Child Related Activities
- Service Standard 1.1.26 Volunteer and Visitor Access to Network Services and Data
- Service Standard 1.1.30 Public Interest Disclosures
- Service Standard 1.4.3 Public Access to Government Information
- Service Standard 1.4.5 Social Media

- Service Standard 1.4.6 Websites
- Service Standard 1.4.8 Media
- Service Standard 2.1.3 Brigade Registers
- Service Standard 2.1.6 Joining the NSW RFS as a Volunteer Member (Inc. Transfer Applications)
- Service Standard 6.1.3 Training in the NSW RFS: SOP 6.1.3 – 14 Records
- Policy P5.1.6 Records Management
- Policy P6.1.4 Bush Fire Hazard Complaints and Notices and associated Guidelines

Service Standards and Policies are developed in consultation with, and distributed to, NSW RFS staff by email and intranet notifications, and to NSW RFS volunteers through the MyRFS web portal.

Service Standards and Policies are reviewed every three years, or earlier where relevant legislation has changed or where an urgent need to revise policies and procedures has been identified. NSW RFS staff and volunteers are notified when policies and service standards have been updated.

New members and existing members transferring Brigades are also informed of privacy rights associated with personal information provided to the NSW RFS via extensive explanatory material in the relevant forms.

8 Raising awareness of privacy obligations

The NSW RFS is committed to complying with the privacy principles set out in PPIPA and HRIPA, and has developed strategies targeted at ensuring compliance is achieved. Strategies implemented to promote general privacy awareness and compliance with privacy obligations include:

- Promotion of the NSW RFS's *Code of Conduct and Ethics*, issued to all staff, which makes provision for how personal and private information collected from other members or the public is to be dealt with
- All staff are required to complete an annual acknowledgment confirming they have read and understand the NSW RFS Code of Conduct and Ethics.
- The requirement for all new staff to take part in an induction program and a one day course on the NSW RFS Code of Conduct and Ethics.
- Consent forms and collection notices are reviewed for new projects and proposals across the NSW RFS.
- When staff perform a role that requires access to personal information, managers have a responsibility to ensure that staff are made aware of their privacy obligations when conducting their work.
- Privacy issues are reported annually in the NSW RFS Annual Report.
- Developing and maintaining the currency of Service Standards, including Service Standard 1.1.14 *Personal and Privacy Information* to guide staff and volunteer compliance with privacy legislation.
- Privacy issues are identified and addressed during the development and implementation of new systems, policies and procedures.
- Informing people about the Privacy Management Plan when answering queries about personal

information.

- Recording and monitoring obligations through the Compliance Management System

8.1 Annual communiqué relating to privacy

Volunteers and staff of the NSW RFS are informed of their responsibilities under privacy legislation via the Service Standards and the Privacy Management Plan. The NSW RFS recognises, however, that there is a need to maintain and periodically update the awareness of volunteers and staff of their obligations and of any changes to the privacy landscape.

To address this need, the NSW RFS has introduced a communications program that involves the dissemination of an annual communiqué on privacy coinciding with Privacy Awareness Week. The contents of the communiqué will be aimed towards raising general awareness of privacy obligations as well as summarising any changes to compliance responsibilities or significant privacy issues affecting the NSW RFS.

The communiqué is distributed through an all staff email and on MyRFS and the Intranet to ensure dissemination across the NSW RFS membership.

8.2 Privacy training and awareness

The NSW RFS will introduce a privacy training and awareness program targeted at managers.

Senior staff will be regularly notified of external privacy training opportunities, conferences, and information sessions which may become available.

In particular, information regarding such training opportunities will be circulated to coincide with communications related to revisions of this Privacy Management Plan. Relevant staff will attend external training to maintain their currency of knowledge.

The NSW RFS will also develop an in house privacy training program for staff of the NSW RFS.

8.3 Review of forms

The NSW RFS uses a number of forms to collect personal information and forms that specifically relate to a function/activity governed by a Policy or Service Standard are reviewed as a component of the policy review process.

To coincide with the periodic revision of this Privacy Management Plan a reminder will be sent to each NSW RFS Directorate to review any such forms the Directorate uses. The NSW RFS Legal and Government Information unit will also conduct a periodic audit of forms to ensure compliance.

9 Privacy complaints and reviews

9.1 Your right to internal review

Section 53 of PPIPA gives a person the right for internal review if they believe that the NSW RFS has breached their privacy. The internal review examines the conduct of the NSW RFS in relation to that alleged breach. In this case, the conduct being examined is whether the NSW RFS:

- Breached one or more of the IPPs or HPPs; or
- Breached a code made under PPIPA (where the code applies to the NSW RFS).

<u>Resolving the matter internally</u>

The NSW RFS encourages people to contact the NSW RFS Privacy Officer (the Manager, Legal and Government Information) in the first instance to discuss any concerns they may have regarding potential

breaches of the IPP's or HPP's involving their personal or health information.

The NSW RFS (subject to the person's consent) will attempt to resolve the issue informally by directing the person's concerns to the appropriate Directorate as part of the NSW RFS' normal complaints handling process.

Internal review

Applications for internal review must be made to the NSW RFS within six (6) months from the date a person becomes aware the alleged privacy breach. Applications must be:

- Made in writing
- Addressed to the NSW RFS Privacy Officer
- Specify an address in Australia where the findings of internal review can be sent.

It is important to note that an internal review can only be requested by a person in relation to a potential breach of their own privacy, unless he or she has authorised another person to act on their behalf.

Applications for internal review can be made using the internal review application form developed by the Information and Privacy Commission. The form can be downloaded at:

https://www.ipc.nsw.gov.au/form-privacy-request-internal-review

Applications should be sent to the NSW RFS Privacy Officer at:

Mail: Locked Bag 17
Granville NSW 2142

Email: legal@rfs.nsw.gov.au

An internal review can only be requested by the person to whom the alleged breach of privacy relates, unless he or she has authorised another party to act on their behalf.

The Privacy Officer will conduct the internal review unless a conflict is identified. If a conflict is found, another person will be appointed to conduct the internal review. Internal reviews conducted by the NSW RFS are done with the co-operation of the Manager of the Unit alleged to be responsible for the breach (the Investigating Manager).

The NSW RFS will:

- Acknowledge receipt of the request for internal review within 5 working days
- Complete the internal review within 60 working days.

Internal reviews will follow the process set out in the Information and Privacy Commission's checklist. When the internal review is completed the applicant is notified in writing of:

- The findings of the review
- The reasons for those findings
- Any action the NSW RFS proposes to take
- The applicant's entitlement to have the NSW RFS' findings reviewed by the NSW Civil and Administrative Tribunal.

The role of the Privacy Commissioner: complaints and internal review

When the NSW RFS receives an application for internal review it must notify the Privacy Commissioner of

the application. The NSW RFS must also:

- Keep the Privacy Commissioner informed of the progress of the internal review
- Advise the Privacy Commissioner of the outcomes of the internal review and any action the NSW RFS proposes to take.

A copy of the draft internal review report must also be provided to the Privacy Commissioner to enable the Commissioner to determine whether to make a submission to the internal review. The NSW RFS must take into account any submissions made by the Privacy Commissioner when finalising the internal review report.

You also have the right to complain directly to the Privacy Commissioner about the NSW RFS' conduct. However, the Privacy Commissioner may decide not to deal with a person's complaint if satisfied that it would be more appropriate for the person to request the NSW RFS to conduct the internal review.

Complaints can be made to the Privacy Commissioner at:

Mail:	GPO Box 7011
	SYDNEY NSW 2001
Email:	ipcinfo@ipc.nsw.gov.au
Telephone:	1800 472 679
Office hours:	9am to 5pm Monday to Friday

9.2 Your right to external review

A person can also apply to the NSW Civil and Administrative Tribunal (NCAT) if:

- They are not satisfied with the NSW RFS' findings of internal review
- They are not satisfied with the action the NSW RFS took in relation to their internal review application
- The NSW RFS has taken more than 60 days to complete their internal review

A person must lodge their application with NCAT **within 28 days** of receiving the NSW RFS' internal review report.

The NCAT has the power to make binding decisions on an external review. The contact details for NCAT are:

Telephone:	9377 5711
Address	Level 10
	John Maddison Tower
	86-90 Goulburn Street Sydney NSW 2000
Website	www.ncat.nsw.gov.au

The NCAT does not provide legal advice, however their website has general information about the process of seeking an external review.

10 Notifiable data breaches

On 22 February 2018, the Notifiable Data Breaches (NDB) scheme under the Commonwealth's *Privacy Act 1998* ('the Privacy Act') came into effect.

The Act provides for the establishment of a mandatory data breach notification scheme that requires agencies covered by the Privacy Act to notify individuals likely to be at risk of serious harm due to a data breach.

While the scheme is largely targeted towards Commonwealth government agencies and private sector agencies regulated by the Australian Privacy Principles under the Privacy Act, there are provisions that apply to NSW public sector agencies.

10.1 Tax File Number Collection

Agencies which collect Tax File Numbers (TFN) will have obligations under the NDB scheme in circumstances where a breach occurs involving a TFN. A TFN data breach occurs where TFN information is lost, or subject to unauthorised access or disclosure (eg where a database containing TFN information is hacked or if a TFN is mistakenly provided to the wrong person).

If a data breach, or an allegation of a data breach arises, the breach will be promptly notified to legal@rfs.nsw.gov.au and ICTServiceDesk@rfs.nsw.gov.au. This is particularly important in cases where IT equipment (RFS issued phones, laptops, and databases) may have been compromised or lost.

In the event of a data breach, Legal and Government Information (LGI) will work with the affected Directorate/s to co-ordinate a response on how the data breach is being dealt with.

Responding to a TFN data breach

The NSW RFS will implement four key steps when responding to a data breach. It will:

1. Contain the data breach
2. Evaluate and mitigate risks to minimise the likelihood that the breach will result in harm to a person
3. Notify the Australian Privacy Commissioner (APC) and the person affected. LGI will work with the relevant Directorate in preparing a statement to the APC containing relevant details about the breach.
4. Prevent future breaches by taking a range of steps, such as a security audit, a review of policies and procedures and training.

The NSW RFS will also report the TFN data breach to the Information and Privacy Commission.

10.2 Sharing Government Sector data

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

If the NSW RFS receives personal or health information under that Act, and it becomes aware that a breach of privacy has or is likely to have occurred, the NSW RFS will inform the data provider and the NSW Privacy Commissioner of the breach.

11 Offences

Sections 62 - 63 of PPIPA and sections 68-69 of HRIPA set out offences in relation to the disclosure and

use of your personal and health information. Staff are made aware of these provisions through privacy training.

12 Reviewing this Plan

This Plan will be reviewed every three years. The Plan will be reviewed earlier if any legislative or administrative changes are made that affect the way personal and health information is managed by the NSW RFS.

13 Appendix A – Implementation Plan

Strategy	Deliverable/s	Responsible Directorate /Unit	Action	Timing
All-staff communication	Communiqué	Legal and Government Information	Research developments in NSW/national privacy landscape	To coincide with privacy Awareness Week (in May each year)
			Draft communiqué	
			Provide to Director, Executive Services for approval	
		Director, Executive Services	Review/approve content	
		Legal and Government Information	Disseminate to all staff (by email)	
Managers' Training Program	Information regarding privacy training	Legal and Government Information	Send all staff email with relevant links to IPC Privacy online Training	To coincide with distribution of the revised Privacy Management Plan
			Research privacy training available	
Review of NSW RFS forms	Forms complying with relevant IPPs and HPPs	Legal and Government Information	Email liaison with NSW RFS Directorates and Policy Unit to develop list of forms	To coincide with distribution of the revised Privacy Management Plan
			Periodic audit of forms	