Service Standard 1.1.14
Personal Information and Privacy

Version	2.6
SOPs	None
Policy Owner	Executive Director Technology, Finance and Legal
Policy Contact	Director Legal and Assurance
Approval Date	12 December 2023
Next Review	28 November 2024

1. Purpose

1.1. The Rural Fire Service (RFS, the Service) values integrity, trust and mutual respect and in order to carry out its functions, collects personal information from both its members and from members of the public.

1.2. The *Privacy and Personal Information Protection Act 1998* (PPIPA) establishes certain principles governing the manner and circumstances in which personal information may be collected and used.

1.3. The *Health Records and Information Privacy Act 2002* (HRIPA) stipulates the responsibilities of private organisations and public agencies in dealing with health information.

1.4. The Data Sharing (Government Sector) Act 2015 governs the sharing of government sector data with a government data analytics centre and between other government agencies and to the privacy and other safeguards that apply to the sharing of that data.

1.5. This Service Standard sets out the manner in which members of the RFS shall collect and use personal information in carrying out the functions of the Service, in order to comply with the provisions of the PPIPA and HRIPA. If there is a conflict between this Service Standard and legislation governing personal information, the legislation shall take precedence.

1.6. The RFS Privacy Management Plan forms part of this Service Standard and further articulates the responsibilities of the RFS under PPIPA and HRIPA.

1.7. The RFS Data Breach Response Plan forms part of this Service Standard and sets out how the RFS will respond to a data breach, including mandatory reporting obligations.

2. Policy

General Principles

Collection

2.1. Personal information shall only be collected or solicited for a lawful purpose that is directly related to a function or activity of the RFS and is reasonably necessary for that purpose.

2.2. Personal information shall be collected from the individual to whom it relates unless:

a. that person authorises the collection of the information from someone else, or

b. the information is collected from the parent or guardian of a person under the age of 16 years.

2.3. Where personal information is collected, the NSW RFS must take reasonable steps to ensure the person providing the information is advised of:

a. the purposes for which the information is being collected

b. the intended recipients of the information

c. the consequences (if any) of not providing the information

d. the person's right to access and correct the information

e. whether the supply of the information is required by law, and the consequences for the individual if the information is not provided, and

f. the name and address of the agency that is collecting the information and the agency that is to hold the information.

2.4. If personal information is collected from an individual then reasonable steps (having regard to the purposes for which the information is collected) must be taken to ensure that:

a. the information collected is relevant to that purpose, is not excessive, and is accurate, current and complete, and

b. the collection of the information does not intrude to an unreasonable extent on the personal affairs of the individual to whom the information relates.

Retention

2.5. It must be ensured that personal information held:

a. is kept for no longer than is necessary for the purposes for which the information may lawfully be used

b. is disposed of securely and in accordance with any requirements for the retention and disposal of personal information

c. is protected by taking reasonable security safeguards (given the circumstances) against loss, unauthorised access, use, modification or disclosure and against all other misuse, and

d. that if it is necessary for the information to be given to a person in connection with the provision of a service to the NSW RFS, that everything reasonably within the power of the NSW RFS is done to prevent unauthorised use or disclosure of the information.

Access and alteration

2.6. A person may:

a. enquire whether the NSW RFS holds personal information about them

b. request access to that information in a reasonable timeframe and without it being costly, and

c. enquire as to the purposes for which it is being held.

2.7. The NSW RFS must, at the request of the person to whom the information relates, make amendments to the personal information to ensure that it is:

a. accurate

b. silent (upon a member’s request)

c. relevant to the purpose for which it was collected

d. up to date

e. complete, and

f. not misleading.

2.8. Volunteer members seeking to make their contact details silent, may do so by:

a. requesting the secretary of their brigade or their district manager to ensure that all appropriate information databases and records are made silent, or

b. registering with OneRFS and following the guided instructions.

2.9. Staff members seeking to make their personal telephone contact details silent may do so by advising:

a. their supervising officer, and

b. Membership Services.

2.10. Any request made pursuant to paragraphs 2.6, 2.7 and 2.8 must be completed within 21 days of receipt. If, for any reason, this is not possible, the matter shall be referred to the Executive Director Technology, Finance and Legal for appropriate action.

Disclosure

2.11. Personal information relating to a person's:

a. ethnic or racial origins

b. political opinions

c. religious or philosophical beliefs

d. trade union membership

e. health, or

f. sexual activities

can only be disclosed if it is necessary in order to prevent or lessen a serious and imminent threat to the life or health of a person or where it is required by law.

2.12. Personal information submitted to the RFS as part of a Bush Fire Hazard Complaint (such as name and address details) shall not be disclosed to anyone outside the RFS. Where disclosure of the complainant's details outside of the RFS is considered necessary for the correct identification of the hazard land, subject to paragraph 3.25, written permission from the complainant must be obtained before that disclosure is made.

2.13. Personal information may be disclosed to another person or body if:

a. the disclosure is directly related to the purpose for which the information was collected and there is no reason to believe that the person concerned would object to the disclosure

b. the person from whom the information was collected is reasonably likely to have been aware or to have been made aware that information of that kind is usually disclosed to that other party, or

c. disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of a person, or

d. it is required to be disclosed by law and/or for law enforcement purposes.

Use of information

2.14. Personal information shall not be used without taking reasonable steps (given the circumstances) to ensure that, having regard to the purpose for which the information is proposed to be used, the information is relevant, accurate, current, complete and not misleading.

2.15. Personal information must not be used for a purpose other than that for which it was collected unless:

a. the person to whom the information relates has consented to the use of the information for that other purpose

b. the other purpose is directly related to the purpose for which the information was collected

c. the information is to be used to prevent or lessen a serious and imminent threat to the life or health of a person, or

d. where it is required to be disclosed by law and/or for law enforcement purposes.

2.16. Health information of an individual must not be intentionally disclosed or used by the RFS, other than in connection with the lawful exercise of its official functions.

Data breach

2.17. All RFS members have a responsibility to report a known or suspected data breach.

2.18. Any known or suspected data breach shall be managed in accordance with the Data Breach Response Plan that forms part of this Service Standard, and RFS ICT standards and protocols.

Privacy Officer

2.19. The designated RFS Privacy Officer is the Manager Legal.

Application of general principles in specific circumstances

2.20. The general principles set out in paragraphs 2.1 to 2.4 and 2.13 to 2.14 inclusive do not apply in relation to the collection and use of personal information relating to or gathered in the course of operational activities, if compliance with the general principle would be impossible or impracticable.

2.21. The RFS is not required to comply with general principle 2.2 if the information concerned is collected in connection with proceedings (whether or not actually commenced) before any court or tribunal.

2.22. The RFS is not required to comply with general principle 2.3 if the information is collected for law enforcement purposes. This does not remove any protections provided by any other law in relation to the rights of an accused person, or person suspected of having committed an offence.

2.23. The RFS is not required to comply with general principles 2.11 to 2.13 if the disclosure of the information concerned:

a. is made in connection with proceedings for an offence or for law enforcement purposes, or

b. is to a law enforcement agency for the purposes of ascertaining the whereabouts of an individual, or

c. is authorised or required by subpoena or by search warrant or other statutory instrument, or

d. is reasonably necessary for the protection of public revenue or in order to investigate an offence where there are reasonable grounds to believe that an offence may have been committed.

2.24. Exemptions may apply to the general principles set out in paragraphs 2.1 to 2.4 and 2.13 to 2.15 inclusive if complying with these principles might detrimentally affect (or prevent the proper exercise of) the RFS complaint handling or investigative functions. Similar exemptions may also apply to information for the purpose of research carried out in the public interest.

2.25. The RFS is not required to comply with the general principles set out in paragraphs 2.1 to 2.4 and 2.13 to 2.15 with respect to the exchange of information between it and other public sector agencies and the collection, use or disclosure of the information if reasonably necessary for law enforcement purposes. This exemption also applies when the information is reasonably

necessary to allow the RFS to respond to ministerial inquiries, to enable inquiries to be referred between agencies, or to enable the auditing of the accounts or performance of the Service.

2.26. Communication systems used by the RFS, including telephones and radios, may record conversation or information provided that:

a. the arrangements for the recording of information are in accordance with Service Standard 5.1.3 Communication Systems

b. the communication system is or may be, used for, or in relation to authorised RFS activities in a lawful manner

c. the manner in which the recording is made complies with any relevant State and/or Federal legislation

d. the recording equipment and recording media, including but not limited to tapes or discs etc., are kept secure

e. a record of a communication is only used for:

i. operational activities

ii. incident debriefing

iii. accident or incident investigation

iv. training

v. where required by law, or

f. records of communications are only accessed with the consent of the Commissioner or the Executive Director Preparedness and Capability unless access to a recording of a communication is required to obtain or confirm information for an immediate operational purpose or for a lawful purpose.

2.27. Personal information that is required in order to contact or communicate with a member of the RFS (e.g. telephone and address lists) for operational or administrative purposes may be collected and disclosed to:

a. members of the brigades to which an individual belongs

b. group officers

c. members of the staff of the RFS, and

d. investigating authorities

who require access to that information in order to carry out their functions.

2.28. Any member of the RFS who is provided with personal information pursuant to the provisions of clause 2.23 must comply with the general principles set out in paragraphs 2.5, 2.12 and 2.14.

2.29. The general principles set out in this Service Standard do not apply to the collection or disclosure of information for the purpose of nominating a member of the RFS for an award or honour, where it would be impracticable to apply that principle.

2.30. PPIPA and HRIPA expressly provide that nothing in those Acts affect the operation of the *Government Information (Public Access) Act 2009* (GIPA Act). This means that personal information held by the RFS may be disclosed in response to a formal access application under the GIPA Act, in order to comply with the Service's obligations under that Act.

The RFS will, where reasonably practicable, consult with the relevant individuals to ascertain if they have any concerns about the release of their personal information and take these into consideration in making a determination in relation to any such access application.

Legitimate use of recordings and surveillance

2.31. The recording of conversations and images is covered by several statutes and must be treated with the utmost privacy and integrity. They shall be replayed or made available only in the following situations:

a. investigation of alleged untimely or inadequate responses to fire or other incidents

b. written inquiries from the NSW Police Force, ICAC, Coroner or other investigating body

c. for the conduct of internal RFS investigations

d. training purposes when prior to recording, consent has been obtained from all parties featured in the audio or video recordings, or

e. as required by law.

2.32. Voice recordings and transcripts of voice recordings obtained through communication systems used by the RFS shall not be used for RFS disciplinary procedures without the express written permission of the Commissioner, Executive Director People and Strategy or Director Performance and Conduct.

2.33. Voice recordings and transcripts of voice recordings obtained during volunteer and staff discipline investigation processes shall only be used for that purpose or associated appeals, and only with the written authorisation of an appropriately delegated authority.

2.34. The use of recorded communications for any other purpose is in most cases prohibited by law, but where required for any other purpose shall only be done with the written approval of the Commissioner. Rapid Recall recordings should only be used for clarification of details passed in a recent conversation.

Alerting Users

2.35. In accordance with SS 5.1.3 Communication Systems, all users shall be made aware of the lines on which calls are being monitored and recorded, and the procedures associated with such recording.

3. Definitions

3.1. For the purpose of this Policy Document, the following definitions apply:

a. **Health Information:** personal information that is information or an opinion about an individual's:

i. physical or mental health or disability

ii. health services (both current and future)

iii. information relating to organ or other bodily part donations, or

iv. genetic information.

b. **NSW RFS communication systems:** the infrastructure, hardware, software and associated devices that enable the NSW RFS to communicate with any party at any time. It includes but is not limited to:

i. fixed and mobile radios

ii. fixed and mobile telephone systems

iii. paging systems

iv. base sites

v. transmission towers

vi. networks used for communication

vii. programming profiles

viii. emergency service voice recording systems

ix. communications data storage infrastructure and equipment, and

x. the procurement, installation, repair, maintenance and disposal thereof.

c. **Personal Information:** information or opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. This includes information forming part of a database, and whether or not recorded in a material form.

4. Document control

Release history

Version	Date	Summary of changes
1.0	17 October 2001	Initial release
2.0	5 November 2004	Repealed and remade SS 1.1.14 v1.0 Complete revision of v1.0
2.1	31 May 2005	Repealed and remade SS 1.1.14 v2.0 Clause 2.2.1 Clause 2.2.9
2.2	23 March 2006	Repealed and remade SS 1.1.14 v2.1 Clause 1.4 deleted Clauses deleted – 2.2.4, 2.2.5, 2.2.7, 2.2.8, 2.2.9, 2.2.11, 2.3.3(a)
2.3	2 November 2007	Repealed and remade SS 1.1.14 v2.2 New section added: Legitimate Use of Recordings – Clauses 2.20-2.23
2.4	4 August 2014	Repealed and remade SS 1.1.14 v2.3 Reviewed to reflect current practices New clause added referring to Privacy Management Plan- clause 1.4 Development of NSW RFS Privacy Management Plan
2.5	20 November 2018	Repelaed and remade SS 1.1.14 v2.4 Removal of Privacy Management Plan from Service Standard Addition of 3.16 to cover section 68 and 69 of HRIP Act Addition of exemptions at 3.18 to 3.22 Addition of training audio and visual recordings at 3.28(d) Addition of tpp 15-03 and DFSI-2016-07 to Related Documents
2.6	12 December 2023	Repealed and remade SS 1.1.14 v2.5 Publication of 1.1.14B RFS Data Breach Response Plan v1.0 Minor updates to 1.1.14A Privacy Management Plan v1.1 to reference 1.1.14B Data Breach Response Plan Update position titles to reflect current organisational alignment

Approved by

Name	Position	Date
Rob Rogers AFSM	Commissioner	12 December 2023

Related documents

Document name
Privacy and Personal Information Protection Act 1998
Health Records and Information Privacy Act 2002
Government Information (Public Access) Act 2009
Telecommunications (Interceptions and Access) Act 1979 (Cth)
Telecommunications (Interceptions and Access) (New South Wales) Act 1987
Surveillance Devices Act 2007
State Records Act 1998
Treasury Policy tpp 15-03 Internal Audit and Risk Management Policy for the NSW Public Sector, Policy and Guidelines Paper, version 1.0
DFSI-2016-07 Privacy Governance Framework – 5 May 2016
Service Standard 1.1.3 Grievances
Service Standard 1.4.8 Media
Service Standard 1.1.7 Code of Conduct and Ethics
Service Standard 1.1.9 Working with Children Check
Service Standard 1.4.4 Volunteer and Visitor Access to Network Services and Data
Service Standard 1.1.30 Public Interest Disclosures in the NSW RFS
Service Standard 1.4.5 Social Media
Service Standard 1.4.6 NSW RFS Websites
Service Standard 2.1.3 Brigade Registers
Service Standard 2.1.6 Volunteer Membership Applications
Service Standard 5.1.3 Communications Systems
Service Standard 6.1.3 Training in the NSW RFS
Policy P5.1.6 Records Management
Policy P6.1.4 Bush Fire Hazard Complaints and Notices

Document name
1.1.14A RFS Privacy Management Plan
1.1.14B RFS Data Breach Response Plan
RFS Website Privacy Statement