NSW RURAL FIRE SERVICE

POLICY P5.1.2
ACCEPTABLE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT)

ITEM	DESCRIPTION
Version Number	2.1
SOPs	› SOP P5.1.2 – 1 Acceptable Use of ICT
Owner	Executive Director, Infrastructure
Contact	Director, ICT
Approved Date	20 August 2019
Effective Date	20 August 2019
Next Review Date	20 August 2024
Document Control	Electronic - Printed Copies are Uncontrolled

1 Purpose

1.1 This policy provides guidance for acceptable use by NSW Rural Fire Service (NSW RFS) employees of NSW RFS Information and Communications Technology (ICT), and on measures to be taken by the NSW RFS.

1.2 This policy applies to NSW RFS staff, contractor users and other authorised individuals. Volunteer and visitor user should refer to SS 1.4.4 Volunteer and Visitor Access to Network Services and Data.

2 Policy

Acceptable Use of ICT and the Intranet

2.1 ICT is provided for business and operational use. Reasonable private use (including for study purposes) is permitted as long as organisational needs take priority.

2.2 NSW RFS members may be required to sign a Conditions of Use agreement when issued with ICT equipment.

2.3 All use, both business and personal, must be lawful, efficient, and ethical. ICT usage is monitored to ensure the appropriate NSW RFS policies and service standards, and Government directives and/or relevant legislation are not contravened. If inappropriate use is identified, access may be withdrawn immediately, and the user may be subject to disciplinary action. Penalties could include termination of employment and/or criminal prosecution.

2.4 The NSW RFS reserves the right to audit, add, and/or remove any illegal material from ICT facilities without notice.

2.5 The computer systems, including the Intranet, shall be accessed by staff, and other authorised individuals as referred in Service Standard 1.4.4 Volunteer and Visitor Access to Network Services and Data.

2.6 Staff requiring access in addition to that already provided, must request it through their Manager and follow ICT standard operating procedures. Where a genuine business reason exists that requires access to facilities or internet sites that would normally be blocked, authorisation may be granted by a manager for a limited period of time.

2.7 The ICT section monitors access and use of the internet and email to ensure that prohibited material is not accessed and that use is reasonable. The Commissioner, Executive Directors, Directors, and Managers reserve the right to undertake spot checks and/or request usage reports from ICT.

2.8 Monitoring, logging and Secure Sockets Layer (SSL) visibility tools are used by the NSW RFS on all ICT systems and services. The user accepts this condition as part of their login conditions to the NSW RFS systems and services.

2.9 District sites with the ability to provide their volunteers with network access through ICT systems should only provide volunteers with network access if they:

a. assist in an IMT role; or

b. are performing tasks requested by their District Manager that require network access.

2.10 Access rights are monitored. If volunteers are assigned inappropriate network access, staff may be subject to misconduct proceedings under the *Government Sector Employment Act 2013* (GSE Act), and volunteers may be subject to disciplinary action. Refer to Service Standard 1.4.4 Volunteer and Visitor Access to Network Services and Data for further details.

2.11 The NSW RFS may monitor, copy, access or disclose information or files that are stored, processed or transmitted using agency equipment and services.

2.12 Where inappropriate use of ICT is identified, the NSW RFS shall act in accordance with the appropriate NSW RFS policies and Service Standards, Government directives and/or relevant legislation.

2.13 In accordance with P5.1.6 Records Management, information, data or records created by NSW RFS staff while employed by the Service are official documents and subject to statutory record keeping requirements.

2.14 Access to NSW RFS networks and systems is governed by user names and passwords. Passwords shall not be divulged to others. Password owners are accountable for any misuse, and divulgence may lead to disciplinary action (for volunteers) or misconduct proceedings under the GSE Act for staff.

2.15 ICT provides a separate service available at most sites for individuals to connect their wireless devices (laptops, smart phones, iPads, tablets, other computing and similar devices) to the internet via a wireless guest internet solution. Access requires a user name and password available from the ICT Service Desk.

2.16 NSW RFS managers who host guests using the guest internet shall ensure, before they connect, that they are briefed on acceptable use.

2.17 ICT provides NSW RFS staff with connectivity to the NSW RFS email solution for approved wireless devices, e.g. laptops, smartphones etc.

2.18 A NSW RFS computer shall not be connected to the internet by any other means (e.g. wireless) when it is also connected to the NSW RFS network.

2.19 When NSW RFS ICT equipment is used outside of the NSW RFS network (e.g. using a laptop at a seminar), it shall be used responsibly (see clause 2.3).

2.20 Network accounts should be requested, approved and validated periodically by managers. All requests must be sent to ICT Service Desk.

2.21 In conforming with NSW Open Data and Data NSW, all data and information published by the NSW RFS should be made available under Creative Commons licensing, using CC BY 3.0 AU as a default, if nothing stricter is required by the content.

Employee and Visitor Responsibilities

2.22 Clear desk and clear screen – Access to NSW RFS information is provided on a 'need-to-know' basis. This means that not everyone is permitted, nor do they require, access to all information. To help ensure information assets remain suitably protected and restricted to those who 'need-to-know'. Information (such as paper records, media, and even soft copy documents that are visible on a computer screen) must not be left unattended or accessible to those without relevant authority.

2.23 All employees and visitors utilising NSW RFS systems have a responsibility to ensure they do not:

a. intentionally create, send or access information that could:

i. Damage the reputation of the NSW RFS;

ii. Be misleading or deceptive;

iii. Result in victimisation or harassment, (which may then lead to criminal penalty or civil liability);

iv. Be reasonably found to be offensive, obscene, threatening, abusive or defamatory;

b. operate a business, take control of NSW RFS business opportunities, or generate personal income (including through gambling);

c. send, receive, print or otherwise disseminate proprietary data, trade secrets or other confidential information of the NSW RFS to unauthorised recipients;

d. gain unauthorised access or make unauthorised changes to programs or data, or otherwise destroy the integrity of electronic based information;

e. develop and deploy applications to any NSW RFS equipment without the express permission of ICT;

f. import or use executable programs into the NSW RFS network or download programs from the Internet without the express permission of ICT;

g. make copies of any software licensed to the NSW RFS, or load any software licensed to the NSW RFS onto personal computers, laptops or servers not owned by the Service; unless specific, written permission obtained from ICT;

h. inappropriately use intellectual property;

i. violate the privacy or rights of other users;

j. use games, streaming multimedia or other non-business, high bandwidth activities not related to agreed roles and/or responsibilities, or without prior approval; or

k. use in any other inappropriate manner, including but not limited to, any use of NSW RFS equipment or services for intentionally transmitting, communicating or accessing pornographic or sexually explicit material, images, text or other offensive material, or any material which may discriminate against, harass or vilify any other person.

Security incident reporting

2.24 Security incidents may occur from time to time. They may arise as a result of non-intentional human error, intentional actions, or through the exploitation of new security weaknesses and vulnerabilities.

2.25 Security incidents must be quickly identified, reported and appropriately managed so that security threats can be contained.

2.26 All staff and contractors must:

a. immediately report identified or suspected information security incidents to the ICT Service Desk; and

b. immediately report identified or suspected information security threats to the ICT Service Desk.

2.27 Information security threats that must be reported include any event or condition that could give rise to a security incident or breach. Examples of information security incidents that must be reported include:

a. ineffective security control;

b. breach of information or ICT system confidentiality, integrity or availability;

c. human errors;

d. non-compliance with the NSW RFS Information Security Policy (this policy);

e. breaches of physical security arrangements;

f. uncontrolled system changes;

g. viruses or unusual information system activity; and

h. malfunctions of software or hardware.

Information security awareness

2.28 Information security awareness develops greater depth in defence of NSW RFS information assets.

2.29 Technical information security mechanisms exist at NSW RFS to secure information assets. Effective information security also requires awareness and proactive support of all staff and contractors that may be targeted by social engineering attacks (i.e. baiting, phishing emails, spam emails, etc.).

2.30 Social engineering attacks and frauds directly target vulnerable humans rather than ICT technologies and network systems. All staff and contractors must participate in and be acquainted with NSW RFS information security awareness programs in order to provide on-going awareness and proactive support for a robust information security framework at NSW RFS.

Employees under Workers Compensation/ Injury Management

2.31 In accordance with P3.4.1 Workers Compensation and Injury Management for NSW RFS Employees, staff who are under Workers Compensation/Injury Management, or Return to Work Programs, are required to adhere to WorkCover Certificate of Capacity restrictions whilst incapacitated for work, including only accessing emails or network for liaison with their Supervisor/Manager or RTW Coordinator.

2.32 The Supervisor/manager of the employee is to evaluate if an injured employee's network access should be limited for health and welfare reasons due to WorkCover Certificate of Capacity restrictions; Any decision to restrict an employee's ICT access is only to be made with concurrence from a Regional Manager or Director.

2.33 The Supervisor/manager of the employee is to consult with the Employee RTW Coordinator if the injured employee has no capacity for work with regard to the employee's work related activities including access to emails and/or network whilst having no capacity for work.

3 Related documents

- *Government Sector Employment Act 2013*
- *Privacy and Personal Information Protection Act 1998*
- *State Records Act 1998*
- NSW DPC Circular 1999-9 Use of Employer Communication Devices
- NSW DPC Protocol for Acceptable Use of the Internet and Electronic Mail
- NSW PSC D19999_007 Policy and Guidelines for the use by Staff of Employer Communication Devices
- Service Standard 1.1.2 Discipline
- Service Standard 1.1.7 Code of Conduct and Ethics
- Service Standard 1.1.14 Privacy and Personal Information
- Service Standard 1.1.19 Intellectual Property
- Service Standard 1.1.42 Respectful and Inclusive Workplace
- Service Standard 1.4.1 Organisational Communication
- Service Standard 1.4.4 Volunteer and Visitor Access to Network Services and Data
- Service Standard 1.4.5 Social Media
- Service Standard 1.4.6 NSW RFS Websites
- P5.1.1 ICT Equipment Standards
- P5.1.3 Information Security Management
- P5.1.6 Records Management
- P3.4.1 Workers Compensation and Injury Management for NSW RFS Employees

4 Amendments

AMENDMENT DATE	VERSION NO	DESCRIPTION
31 March 2009	1.0	Initial release
2 June 2011	1.1	› Repealed and remade P5.1.2 v1.0 › Addition of clauses 2.11 and 2.18(e)
10 October 2013	1.2	› Repealed and remade P5.1.2 v1.1

AMENDMENT DATE	VERSION NO	DESCRIPTION
		› Reviewed to incorporate 2.1.3 Intranet Content Development and Management and reflect current practices
4 May 2017	2.0	› Repealed and remade P5.1.2 v1.2 › Reviewed and updated to include recommendations from Information Security Management Systems audit
20 August 2019	2.1	› Repeals and remakes P5.1.2 v2.0 › Added clauses to further address information security – clauses 2.22, 2.24-2.30

SOP P5.1.2-1
ACCEPTABLE USE OF ICT

1 Purpose

1.1 This Standard Operating Procedure (SOP) details the procedures the NSW RFS has implemented to ensure acceptable use of ICT.

2 Procedures

Definitions and abbreviations

2.1 For the purpose of this Policy, the following terms apply:

a. **IMT:** Incident Management Team

b. **ICT:** Information and Communication Technology

c. **SAP Enterprise Asset Management (SAP EAM):** the current NSW RFS asset management System

d. **MyRFS:** the volunteer Extranet

Monitoring activity

2.2 ICT may request members of staff to sign a Conditions of Use agreement when issued with, or using ICT equipment.

2.3 The Commissioner, Executive Directors and Directors may request activity reports from ICT that track an individual's ICT usage. These reports track sites accessed and duration of the site visits and can be provided by the ICT service desk on written application. Further details are available from ICT.

Staff and contractor access

2.4 Staff and contractors requiring access to NSW RFS ICT are processed following standard ICT procedures.

2.5 Security is enforced for all staff and contractor accounts with automated, scheduled validation specified in the ICT procedures.

2.6 Where appropriate, ICT will request the manager's name and an assignment end date to determine who validates access on an ongoing basis and when the access expires or requires renewal. The standard access period is three months.

2.7 ICT will provide managers with an expiry notification prior to access being disabled.

2.8 Management should regularly brief new staff, guests and contractors on acceptable use of ICT and the requirement to comply with all NSW RFS policies and procedures.

2.9 The ICT Service Desk only provides wireless guest network access usernames and passwords to NSW RFS managers by request.

Network access for volunteers assisting in an IMT

2.10 District staff can assign network access to a volunteer's MyRFS username through SAP. Refer to Service Standard 1.4.4 Volunteer and Visitor Access to Network Services and Data for further details.

2.11 It is the responsibility of the district staff to reinstate the IMT network access in SAP each year during the pre-season planning process.

ICT Equipment

2.12 All ICT equipment used should conform to the standards specified in policy P5.1.1 Equipment Standards.

3 Related forms

› None