NSW GOVERNMENT

NSW RURAL FIRE SERVICE

POLICY P4.1.9

COMMUNICATIONS – MOBILE AND DATA DEVICES

ITEM	DESCRIPTION
Version Number	1.0
SOPs	› SOP P4.1.9-1 Use and Security of Devices › SOP P4.1.9-2 Purchasing and Replacement of Devices › SOP P4.1.9-3 Disposal, Transfer or Other Changes to the Custodian of a Device
Owner	Executive Director, Technology, Finance & Legal
Contact	Director, ICT
Approved Date	22 June 2021
Effective Date	22 June 2021
Next Review Date	22 June 2026
Document Control	Electronic - Printed Copies are Uncontrolled

1 Purpose

1.1 Communication and data devices in public sector agencies are provided primarily for business use. As public officials, NSW Rural Fire Service (NSW RFS) members are accountable for the manner and purpose for which all public resources are used, i.e. to be efficient, economical and ethical in the use and management of any such resources, including mobile phones and data devices

1.2 Efficient and effective communication is important in the day-to-day running and operations of the NSW RFS.

1.3 All NSW RFS members are required to adhere to this policy which covers issues relevant to the use of NSW RFS issued devices including the purchase, usage, safety and security of communications, data and cost management matters such as cost centre charging.

2 Definitions

2.1 For the purpose of this policy document, the following definitions and acronyms apply:

a. **Devices:** Include smartphones, tablets and similar electronic data devices with a SIM

b. **IMEI:** International Mobile Equipment Identity

c. **MDM:** Mobile Device Management

d. **PIN:** Personal Identification Number

e. **SIM:** Subscriber Identity Module (includes e-Sim)

3 Policy

3.1 All devices that are supplied to NSW RFS members are owned by the NSW RFS. As such, any information stored on the device may be the intellectual property of the NSW RFS / NSW Government.

3.2 Communication/data devices and services are purchased, connected and issued on the approval of the relevant Director against a cost centre.

3.3 NSW RFS allocates devices to NSW RFS members on the basis of their role, duties performed and business activity requirements.

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

3.5 Devices will not be transferred to other entities or to individual's private accounts from the NSW RFS.

3.6 Telephone numbers may be transferred to other entities or individual's private accounts from the NSW RFS at the discretion of the relevant Director.

3.7 The NSW RFS reserves the right to monitor the use of devices and/or data services issued to members.

3.8 Where the use appears to be excessive or in contravention of NSW RFS expectations (refer to the document Acceptable Use of NSW RFS Issued Phones and Data Devices), the Manager should confer with their Director or Area Commander for review and advice.

3.9 NSW RFS members should make all reasonable efforts to become knowledgeable in the proper operation and use of the device(s) before commencing use of the equipment. See SOP P4.1.9-1 Use and Security of Devices for details.

3.10 Members must ensure that all use is lawful and ethical.

3.11 In using NSW RFS supplied devices, all NSW RFS members have a responsibility to ensure steps are taken to maintain the confidentiality of information displayed on the device.

Personal Use

3.12 Reasonable personal use is permitted as part of the NSW RFS commitment to being a responsive and flexible organisation which recognises that members have family and community responsibilities. Such personal use must be reasonable and must not involve activities that conflict with the NSW RFS Code of Conduct, are controversial or offensive.

3.13 Personal use does not include secondary employment and other commercial activities.

International Roaming

3.14 If a NSW RFS member is travelling overseas, they are able to have their device(s) activated to 'international roaming'.

3.15 Members should refer to Premier's Memorandum C2016-04 *Information Security for Ministers, Minister's Staff, Department Secretaries and Senior Executives Travelling Overseas*, which provides an information security framework for members when travelling overseas, with the aim of protecting digital information, NSW Government IT networks and the reputation of the NSW Government.

3.16 The NSW RFS member needs to obtain their Director's approval by completing the relevant section in the Mobile Device Connection Form, and then sending the form to telephone@rfs.nsw.gov.au at least two weeks prior to the NSW RFS member travelling overseas. Pertinent information as to departure and return dates need to be advised to enable 'international roaming' including travel pass and international data plan.

Safety Guidelines

3.17 NSW RFS members must take whatever reasonable precautions are necessary to ensure compliance with the law and their own safety when using communication and data devices, for example while operating a motor vehicle (or any other plant, appliance or vehicle) or when travelling on foot.

3.18 NSW RFS members are expected to comply with all Work Health and Safety requirements and any guidelines issued on the safe use of devices, and to ensure that rules of safety are adhered to.

Replacement lifecycles

3.19 The ordering of replacement devices shall be in accordance with the procedures outlined in SOP P4.1.9-2 Purchasing and Replacement of Devices.

Reporting lost, stolen or damaged devices

3.20 NSW RFS members must as soon as practical contact the ICT Service Desk by phone 1800 00 5123 or via email servicedesk@rfs.nsw.gov.au if their device(s) is lost or stolen. This will allow for the device to be remotely wiped over the network via MDM. Please note that this process will only occur during operating hours - 7.30 am to 10.00 pm Monday to Friday and 10.00 am to 6.00 pm weekends and public holidays.

3.21 NSW RFS members are responsible for managing, blocking and/or removing any personal apps, services or subscriptions on NSW RFS owned devices that have been lost, stolen or damaged,

3.22 NSW RFS members must also notify their Manager or District Manager of the lost/stolen/damaged device, as soon as possible. This notification must also include a written report outlining the circumstances of loss or damage.

3.23 If the device is lost or stolen, the NSW RFS member of the device must also contact the relevant local Police (in most circumstances, NSW Police) to report and obtain an incident / event number. The report/event number must be sent to telephone@rfs.nsw.gov.au together with a copy of the written report, endorsed by the Manager or District Manager, as outlined in Clause 3.22. The report can be made via NSW Police Assistance on 131 444 or *https://portal.police.nsw.gov.au/s/lost-property-definition?reportType=CP_Lost_Property*

Disposal, Moves or Changes to the Custodian of any Device

3.24 It is incumbent on both the Manager and the NSW RFS member to ensure that all relevant corporate asset systems (e.g. SAP and SAP EAM) are updated with the current information to ensure accuracy with regards to:

a. the custodian of the device(s); and

b. if the device is being transferred to another NSW RFS member or section, that this transfer is captured and updated.

3.25 If extended leave is taken, or when leaving a position, the NSW RFS member must ensure that:

a. they return the device to their Manager in accordance with SS 5.2.2 Return of Equipment Allocated to Members of the Service; or

b. where the NSW RFS member changes functions or cost centres, the NSW RFS member must ensure either the outgoing Manager or the incoming Manager advise telephone@rfs.nsw.gov.au of the transfer to facilitate a move in cost code and service records.

3.26 Refer to SOP P4.1.9-3 Disposal, Transfer or Other Changes to the Custodian of a Device.

Data and System Security

3.27 All NSW RFS members shall abide by NSW RFS Policy P5.1.3 Information Security Management at all times.

3.28 All organisational data that is stored on the device must be secured using ICT mandated physical and electronic methods at all times. NSW RFS members must take preventative measures to protect NSW RFS data and systems as detailed in SOP P4.1.9-1 Use and Security of Devices.

4 Related documents

- *Privacy and Personal Information Protection Act 1998*
- *State Records Act 1998*
- NSW DPC Circular C2016-04 Information Security Policy for Ministers, Minister's Staff, Department Secretaries and Senior Executives Travelling
- Policy P4.1.1 Financial Delegations
- Policy P4.1.3 Procurement
- Policy P5.1.1 ICT Equipment Standards
- Policy P5.1.2 Acceptable Use of Information Communications and Technology (ICT)
- Policy P5.1.3 Information Security Management
- Policy P5.1.6 Records Management
- 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

5 Amendments

AMENDMENT DATE	VERSION NO	DESCRIPTION
16 July 2004	*1.0*	› *Initial release as policy 3.1.1 Communications*
25 January 2008	*1.1*	› *Repeals and remakes policy 3.1.1 Communications v1.0* › *Clauses 2.4, 2.5 and 3.2 – minor amendments* › *Updates to align with current role titles and processes*
22 June 2021	1.0	› Updates and repeals Policy 3.1.1 Communications v1.1 › Renumbered and retitled - P4.1.9 Communications – Mobile and Data Devices v1.0 › Comprehensive update, including change of policy owner and contact

SOP P4.1.9-1

USE AND SECURITY OF DEVICES

1 Purpose

1.1 This section details the use and security of NSW RFS devices.

2 Procedures

General Use

2.1 NSW RFS members should familiarise themselves with and utilise one or more of the various security devices available for the device e.g. device PIN code locks, biometrics and other access controls to avoid unauthorised use in the event of loss or theft.

2.2 It is a requirement for all communication devices to be enrolled in the current Mobile Device Management (MDM) system activated through the ICT Service Desk. MDM enables the NSW RFS to push and pull information from each device, including:

- Security policies (such as PIN enforcement);
- Facilitate remotely wiping the device of data if lost or stolen;
- Installing Applications; and
- Email and network settings.

2.3 NSW RFS members are required to comply with all relevant agency or Government guidelines and legislation in respect to transmitting or receiving information which: could damage the reputation of the NSW RFS; could be misleading or deceptive; or could be regarded as being offensive, defamatory or containing material which could amount to sexual harassment, racial harassment or vilification.

2.4 NSW RFS members must not use a NSW RFS device for private commercial activities (even if reimbursement is being provided), or for political party or political campaigning purposes, or for accessing fee-incurring information services for unofficial or unnecessary purposes.

2.5 NSW RFS members should be aware of agency guidelines and, where relevant, Government guidelines and laws in respect to the use and security of communications devices. This includes the unauthorised recording of conversations and the treatment of personal and confidential information. These guidelines must be complied with at all times.

2.6 NSW RFS members who wish to receive NSW RFS information (such as corporate emails and network access) on their personal devices must enrol into the MDM system (refer to clause 2.2).

2.7 All private use of data through the device at home must be through personal internet connections and must be undertaken in line with this SOP.

Security

2.8 All organisational data that is stored on the device must be secured using ICT mandated physical and electronic methods at all times. NSW RFS members must take the following physical security preventative measures to protect NSW RFS data and systems:

a. Device custodians must comply with directives from ICT to update or upgrade system software (or delay upgrades as advised) and must otherwise act to ensure security and system functionality.

b. Downloading applications from the platform’s (e.g. Apple's, Android’s) official, trusted application store is acceptable, as long as the application complies with the 'NSW RFS acceptable use policy' and the NSW RFS Code of Conduct.

c. If official applications, with an approved business use case, have an associated organisational fee, then the custodian of the device must have this approved by their Manager.

d. NSW RFS security policy will be implemented via MDM and may include, but is not limited to, areas such as pass-code, pass-code timeout, pass-code complexity, biometrics and encryption.

e. Jailbreaking, rooting, tampering with boot loaders or any other attempt to bypass manufacturer or carrier limitations of devices or services represents a breach of this policy and Service Standard 1.1.2 Discipline will apply.

2.9 NSW RFS members will be responsible for all transactions made with their credentials, and should not share individually assigned passwords, PINs or other credentials.

3 Related forms

- None

SOP P4.1.9-2

PURCHASING AND REPLACEMENT OF DEVICES

1 Purpose

1.1 This section details the processes for the purchase and replacement of devices.

2 Procedures

2.1 NSW RFS provides devices as a tool of trade. All devices are to be purchased through the NSW RFS procurement solution.

2.2 NSW RFS members seeking to purchase devices outside of this process require written exemptions from their relevant Director.

2.3 All current NSW RFS devices have an Original Equipment Manufacturer (OEM) hardware lifespan of a minimum 24 months.

2.4 Accessories are only to be replaced if not compatible with the new device or if they are non-functional. If accessories are compatible with another device in your business unit that has not reached its expiry, these accessories may be redeployed.

2.5 Managers will establish if the device(s) are appropriate to be reissued or to be disposed.

2.6 All hardware is controlled under the SAP EAM asset register.

Purchasing of Communication Devices

2.7 The relevant Category Manager will ensure that all devices used are fit for purpose and available on the SAP Procurement system.

2.8 The NSW RFS member requesting the device must:

a. check with their Manager if a serviceable device (i.e. second hand device) is available, to be issued prior to the procurement of any new device;

a. if a serviceable device is not available, arrange for a purchase order to be raised in SAP Procurement system;

b. for a new device which has not been connected previously, an approved Mobile Device Connection Form should be sent to telephone@rfs.nsw.gov.au to arrange a SIM card and connection;

c. when the device(s) is received, ensure SAP goods receipt is undertaken and the device IMEI and serial number (and other relevant details) are captured within SAP EAM.

2.9 Costs of purchasing communication and data devices and accessories will be met by the requesting cost centre.

2.10 Car kits and other accessories may be purchased at the same time as the devices. The approval to purchase these kits or accessories will be based on consideration of the NSW RFS member's requirements and role and agreed to by the relevant Director/Area Command Manager.

2.11 Once the communications/data device(s) is received the NSW RFS member should work with ICT Service for the MDM to be configured, profiled registered or updated.

2.12 With respect to damaged devices, broken screens etc., an email should be sent to telephone@rfs.nsw.gov.au who will advise on the best resolution for the repair or replacement of the device.

3 Related forms

- Mobile Device Connection Form

SOP P4.1.9-3

DISPOSAL, TRANSFER OR OTHER CHANGES TO THE CUSTODIAN OF A DEVICE

1 Purpose

1.1 This section details the processes relating to the disposal or transfer of a device, and any changes relating to the NSW RFS member who is the custodian of a device.

2 Procedures

2.1 Mobile phones and data devices may be disposed of when they are more than 24 months old or are no longer serviceable.

2.2 Where the NSW RFS member changes functions or cost centres, the NSW RFS member must ensure the responsible Manager advises telephone@rfs.nsw.gov.au of the transfer to facilitate a move in cost code and service records;

2.3 With respect to disposal of devices, the NSW RFS member is to ensure that:

a. the device is wiped of data as per the Original Equipment Manufacturer (OEM) process

b. SAP EAM is updated to un-allocate the device from the NSW RFS member or have it removed from list of equipment for the NSW RFS member;

c. complete the Mobile Phone and Data Device Disposal Form, located on the NSW RFS Intranet; and

d. email the form to telephone@rfs.nsw.gov.au and forward the device, with a copy of the form, to NSW RFS Glendenning Warehouse.

3 Related forms

- Mobile Phone / Tablet Disposal Form