



WACHS Mobile Device Policy

1. Background

The purpose of this policy is to:

- ensure WA Country Health Service mobile device assets are uniformly and appropriately procured, provisioned and managed
- implement a uniform and consistent approach to device security
- ensure that all users of WA Country Health Service mobile devices are aware of their responsibilities.

2. Policy Statement

This policy is binding upon WA Country Health Service (known hereafter as “WACHS”) and its staff.

In addition, WACHS must ensure that in contracting with Contracted Health Entities, vendors or third parties, the provider and any of their personnel using WACHS owned mobile devices must comply with all relevant mandatory requirements listed in this policy. This includes any person working in a permanent, temporary, casual, contracted, termed appointment or honorary capacity.

This policy covers all mobile devices owned by WACHS including (but not limited to):

- standard mobile telephones
- smart phones (e.g. iPhones, Android phone)
- tablet devices (e.g. iPads, Samsung Galaxy tab)
- laptops (includes notebooks and netbooks).

2.1. Eligible Criteria

The following eligibility requirements must be demonstrated within an application for procurement or provisioning of a mobile device for WACHS staff:

- Mobile devices are only to be allocated to WACHS staff where a genuine business need can be demonstrated for all such devices.
- Requests for mobile devices must be authorised by a Tier 4 or above delegated officer as defined within the [WA Country Health Service Authorities Schedule](#).
- Where the request has been made for a smartphone, tablet, laptop or other data enabled device, approval must be gained from the Director of Information Management and Technology or the ICT Area Operations Manager. In addition, part of the eligibility should include a focus on the laptop/notebook becoming the primary computing device for clinical and non-clinical staff categories avoiding duplication of primary computing devices and licensing.
- A user with a demonstrated business need for multiple mobile devices should only have one mobile data plan.

WACHS Mobile Device Policy

- Tablet Computing Devices, Notebooks, Laptops and Smartphones may be considered where there is a service and/or effectiveness and efficiency gain, and in those instances where the device is used as a clinical tool for:
 - Tier 5 and above
 - clinical and non-clinical staff who routinely (three of five days, or greater than 22 hours/week) undertake travel away from the office
 - clinicians and service providers that can demonstrate consumer benefit and/or greater effectiveness or efficiency in providing care or undertaking their role subject to:
 - funding availability and cost effectiveness
 - the application addressing an identified priority health issue for the region or area.

2.2. Procurement

Mobile devices are issued for business purposes and remain the property of WA Country Health Service. Procurement of all mobile devices, voice & data services (hardware and network carrier), shall be managed by designated WACHS Information and Communication Technology (ICT) staff and in accordance with the Department of Finance guidelines and Common Use Agreements.

Where high-volume mobile data usage is required (e.g. videoconferencing or work related video applications), staff should consult with ICT to ensure adequate data has been procured.

Procurement requests for mobile devices must be made using an:

- Authority and Request for IT Related Hardware/Software/Services form ([HFN-070](#)) where the request is for a laptop or tablet device.
- Authority and Request for Telecommunications Equipment ([HFN-80](#)) where the request is for a mobile phone , smart phone or 4G-enabled tablet.

The business case must demonstrate eligibility criteria and identification of an authorised funding source for initial procurement and on-going billing.

Completed request forms should be scanned and saved in HP Records Manager and lodged with ICT using the established protocols and processes for logging of service requests.

2.3. Personal Use

- WACHS provided mobile devices are primarily for business use. Users should avoid excessive personal use.
- Reasonable Personal use of the mobile telephone is defined in the [MP 0066/17 - Acceptable Use of Information and Communications Technology Policy](#) and is as follows:
 - Reasonable personal use of ICT resources is permitted by staff members where ICT resources are already provided for work purposes. Personal use of ICT resources are activities conducted for purposes other than accomplishing your official duties. In all cases, reasonable personal use must not result in

WACHS Mobile Device Policy

loss of productivity, not interfere with official duties or not result in more than 'minimal additional expense' to the WA health system.

- Staff must support efforts to manage device operation costs by ensuring that call minutes, text messages and data usage do not exceed usage plan limits. Mobile device users are responsible for understanding the specifics of their device plan and manage any reasonable personal use within plan limits.
- Personal use during work time must be kept brief and preferably made during work breaks.
- WACHS mobile users must know what mobile plan they are on. This information will be supplied by your local ICT Telecommunications Coordinators. Significant use in excess of the allocated mobile plan may result in direct recovery of costs from the staff member.
- Personal use of mobile data that is part of the WACHS mobile telephone account must be carefully managed. Streaming of video, or downloads (including applications) consuming large amounts of data utilising the WACHS mobile account data plan is not permitted.
- Users can and should connect devices to personal data plans by connecting to home Wi-Fi etc. where available for personal use.
- Mobile applications and services can be installed but care must be taken not to utilise excess data on the WACHS mobile data account. Where possible, personal applications should be downloaded using personal data plans such as home Wi-Fi etc. Care must be taken not to not breach any legal, ethical or policy standards in relation to the type and nature of applications being downloaded. WACHS retains the right to remove applications and their related content without notice or warning.
- Mobile applications such as email, weather, banking, news, reasonable internet access and social media are acceptable. Social media applications must however, be used strictly within the guidelines of the [WACHS Social Media Policy](#).
- Mobile applications involving any illegal activity or content not meeting the Public Sector Commission ethical standards are not an acceptable use of a work supplied devices and would be considered misconduct.
- Users are responsible for backing up any personal data.

2.4. Service Management, Monitoring and Compliance

Laptops will be managed through the managed operating environment. Mobile Device Management (MDM) software will be used for monitoring and management of mobile voice and data services including all smartphones and tablet devices. The MDM system is to be administered by WACHS ICT delegated officers to:

- manage handset configuration through policy enforcement (restrictions on use), mobile application deployment, locking and fault management
- provide location management and allow immediate disabling of a device that has been lost or stolen
- provide asset management including assignment of devices to organisational structures or individuals
- provide internet content management including whitelisting and blacklisting of websites and services

WACHS Mobile Device Policy

- allow reporting on the data usage on the services to allow identification of possible unacceptable use patterns
- allow forensic and historical information for investigation purposes by the WACHS Integrity Unit where possible misconduct may have occurred.

Monthly use reports are to be generated for inclusion in:

- Executive summary reports
- manager reports on subordinate staff usage
- compliance and integrity audits at a handset and organisational unit level.

2.5. Hardware Requirements

For smartphone and tablet purchases, only procurement requests for supported handsets meeting the minimum required hardware, operating system level will be allowed. This is to ensure all smart phones and tablet devices:

- are compatible with the full suite of management tools available in the Mobile Device Management system
- allow support staff to effectively deliver services such as device and fault management, end-user support and security configuration
- ensure devices have adequate hardware to support encryption of the device.

3. Definitions

MDM	Mobile Device Management
------------	--------------------------

4. Roles and Responsibilities

WACHS staff issued with a mobile device, are bound by legislative and policy requirements defined within:

- [MP 0066/17 - Acceptable Use of Information and Communications Technology Policy](#)
- [MP 0067/17 - Information Security Policy](#)
- WA Public Sector Commission [Code of Ethics](#)
- [Public Sector Management Act 1994](#) (the Act) principles of public administration and management, human resource management and conduct
- [WA Health Social Media Guidelines](#).

Responsibilities and obligations pertaining to WACHS mobile devices include but are not limited to:

- When the mobile device is allocated, the user assumes responsibility for the physical security of the equipment and information contained within. Reasonable steps must be taken to secure mobile devices and use them in ways, situations and applications they are designed for. Staff may be held personally liable for any loss or damage (other than normal wear and tear) to devices and associated costs incurred by the organisation as a result.

WACHS Mobile Device Policy

- Mobile devices must not be left in plain view in an unattended vehicle, even for a short period of time. Devices must not be left in a vehicle overnight.
- A mobile device displaying sensitive information being used in a public place (e.g. train, aircraft or coffee shop) must be positioned so that the screen cannot be viewed by others.
- Mobile devices should not be left unattended unless in a secure environment.
- Mobile devices are a valuable tool in conducting business. It is the policy of WACHS to protect and maintain user safety, security and privacy, while protecting enterprise information assets while using these tools. Use of mobile devices supplied by and funded by WACHS is to primarily be for business purposes.
- Appropriate use is in accordance with state and federal legislation, organisational integrity, conduct and acceptable use standards.
- All staff assigned or last in possession of a WACHS owned mobile device that is lost, damaged or stolen, must immediately advise their line manager and call the appropriate ICT Helpdesk to advise of the loss or damage. Failure to apply due diligence to the reporting of a lost or stolen device may result in a requirement to reimburse WACHS for costs incurred on calls or data made via the device during the period that the staff member was not in possession of it.
- All issued devices must be returned by staff in a timely manner on the termination of their employment with WACHS, transfer of position (following discussion with line manager), or if otherwise directed to do so by their line manager. The line manager must notify ICT.
- Staff must not interfere with mobile device management such as disabling virus protection, security software patches or software updates. WACHS devices may not be modified or altered, including modification of handset IMEI identification, parts, repairs, associated device SIM cards and Health applications.
- Mobile devices must not be utilised while driving unless via hands free.
- Windows devices such as Laptops must be connected to the Health network at least once a month to ensure updates are installed.
- All WACHS staff assigned a mobile or smart phone/tablet device, must comply with the *WACHS Mobiles Telephone Conditions of Use*.
 - On smart phones and tablet devices, these conditions of use will be presented and accepted electronically by the user at the time of handset receipt directly on the device through the mobile device management platform.
Non-acceptance will result in disablement of the device.
- All standard “non-smart” devices require completion of the paper pro-forma. This form must be lodged with the regional ICT Telecommunication Coordinator for recording. Where a shared or pool phone has been issued, all staff members that may use the device need to complete the *WACHS Mobile Telephone Conditions of Use* form.
- The capturing, storage and transfer of patient information and media on mobile devices must be minimised, with the use of secure medical illustrations / photography services, devices and applications provided by WACHS to be used where reasonably practical.

5. Compliance

Failure to comply with this policy may constitute a breach of the WA Health Code of Conduct (Code). The Code is part of the [Integrity Policy Framework](#) issued pursuant to section 26 of the [Health Services Act 2016](#) (WA) and is binding on all WACHS staff which for this purpose includes trainees, students, volunteers, researchers, contractors for service (including all visiting health professionals and agency staff) and persons delivering training or education within WACHS.

WACHS staff are reminded that compliance with all policies is mandatory.

6. Records Management

All WACHS corporate records must be stored in the approved Electronic Documents and Records Management System.

[Records Management Policy](#)

7. Evaluation

This procedure will be evaluated and reviewed every five (5) years from the effective date (or in response to changes to interdependent policies and the environment) by the WACHS Information Governance Committee.

8. Standards

[National Safety and Quality Health Service Standards](#) - 1.16, 1.25

9. Legislation

[Public Sector Management Act 1994](#)

10. References

[State Supply Commission Value for Money Policy](#)

11. Related Forms

Authority and Request for IT Related Hardware/Software/Services form ([HFN-070](#))

Authority and Request for Telecommunications Equipment ([HFN-80](#))

12. Related Policy Documents

[WACHS Social Media Policy](#)

13. Related WA Health System Policies

[Acceptable Use of Information and Communications Technology Policy \(MP0066/17\)](#)

[Information Security Policy \(MP0067/17\)](#)

[WA Health Social Media Guidelines](#)

14. Policy Framework

[Information and Communications Technology Policy Framework](#)

**This document can be made available in alternative formats
on request for a person with a disability**

Contact:	WACHS ICT Operations Manager (S. Halligan)		
Directorate:	Innovation & Development - ICT	EDRMS Record #	ED-CO-13-65557
Version:	4.00	Date Published:	18 June 2020

Copyright to this material is vested in the State of Western Australia unless otherwise indicated. Apart from any fair dealing for the purposes of private study, research, criticism or review, as permitted under the provisions of the *Copyright Act 1968*, no part may be reproduced or re-used for any purposes whatsoever without written permission of the State of Western Australia.