SESLHD POLICY COVER SHEET

NAME OF DOCUMENT	Mobile Services – provisioning and use of
TYPE OF DOCUMENT	Policy
DOCUMENT NUMBER	SESLHDPD/300
DATE OF PUBLICATION	August 2019
RISK RATING	Low
LEVEL OF EVIDENCE	Standard 1 – Clinical Governance
REVIEW DATE	August 2024
REFERENCE(S)	PD 071
EXECUTIVE SPONSOR or EXECUTIVE CLINICAL SPONSOR	Flora Karanfilovski Director Health ICT/CIO
AUTHOR	Linda Nguyen Mobile Service Co-ordinator
POSITION RESPONSIBLE FOR THE DOCUMENT	Linda Nguyen Mobile Service Co-ordinator Linda.Nguyen3@health.nsw.gov.au
KEY TERMS	Mobile phones, smart phones, mobile service
SUMMARY	This policy outlines the process that employees must follow for the acquisition and use of a mobile device and/or service.

Mobile Services – provisioning and use of SESLHDPD/300

1. POLICY STATEMENT

This policy outlines the process that employees must follow for the acquisition and use of a mobile device and/or service.

This includes compliance with Health ICTs (ICT) policies, approval processes and adherence to the underpinning contract by South Eastern Sydney Local Health District's (SESLHD's) third party service provider, Telstra.

2. AIMS

To define the rules, security and usage guidelines to assist with provisioning and management of corporate issued mobile devices and services.

3. TARGET AUDIENCE

All SESLHD entities, managers and employees using or provisioning requests for mobile devices and or services.

4. RESPONSIBILITIES

4.1 Employees will:

- Ensure they are familiar and comply with this policy, as applicable.

4.2 District/Service/Line Managers will:

- Ensure staff are aware of and comply with this policy, as applicable.

5. POLICY

5.1 Standard Requests

A mobile service and a corresponding device, are provided to employees in circumstances where there is a business requirement to fulfil their role as described in their position description. Justification of a mobile phone purchase needs to be clearly defined in the request form and will be reviewed as appropriate.

5.2 Non-Standard Requests

If a non-standard device is requested, that is a physical device that is not part of the standard service catalogue, a third level approval process must be followed. The third level approver is the ICT Director or the Chief Executive. Requests will be considered on a case by case basis without precedent, but in all cases include whether the device is supported by ICT's technical resources. Business justification for the non-standard device will also be validated as part of the approval criteria.

5.3 Replacements Requests

5.3.1 Devices damaged

It is acknowledged that devices may require repair, replacement or become lost due to circumstances beyond an employee's control.

Any damage, loss or theft of a device must be reported immediately to the employee's cost centre manager and the State Wide Service Desk (SWSD).

NOTE: ICT provides no guarantee for retrieving or restoring any personal or SESLHD information, or data stored on the device that may be lost, deleted or compromised.

If the device requires repair, approval will be sought from the employees cost centre manager. The manager is to decide who is liable for meeting the cost of a repair or replacement. This cost may be directed to the employee if it is considered that the damage/loss was incurred through careless or inappropriate action. This includes devices replaced/repaired more than three times in a 12 month period.

5.3.2 End of life replacements and device beyond repair

Devices will be replaced as per section 5.1 or 5.2, as appropriate.

5.4 Procedure

Procedure to provision and use of a mobile device and/or service on the SESLHD network is contained in SESLHDPR/645 Mobile Services – Procedure.

5.5 Approvals

All requests will be reviewed upon submission to ensure all approvals meet audit and compliance.
All requests require cost centre manager and GM/Director approval.
iPhones will be provisioned for Tier 2 executives only, or at Tier 2 discretion.

5.6 Provisioning

Provisioning is managed by the ICT Service Management Team.

Orders will be placed by the Mobile Services Coordinator via Telstra's online portal. The portal provides information on stock availability, current pricing, order status and history. The tool also provides a record of all valid authorised users across the mobile service account.

5.7 Cost inclusions

The monthly charge for each mobile service voice plan includes:

- National and mobile telephone calls,
- National SMS,
- MessageBank diversion
- MessageBank retrieval
- 1300 calls

5.8 Cost exclusions

Charges **not** included on standard mobile voice plans include:

- International calls
- International SMS
- Premium SMS/MMS (see ACMA website for examples)
- Diversions to a landline or mobile number
- 1800/Directory Assistance calls

5.9 Additional services

5.9.1 International Voice Roaming and Data usage

International roaming and data services are not provisioned at the commencement of the service.

International roaming and data services will be granted on a request by request basis. A Mobile/Smart Phone International Roaming Application Form will need to be completed with the appropriate approval. Access will be enabled for a specific duration – i.e. a specified date range from the arrival date to the departure date of the business trip. This form must be provided to Mobile Service Co-ordinator at least one business day before departure date. Usage charges vary according to Telstra's specified zones.

5.10 Transfer of ownership

The SWSD is to be advised of any transfers of ownership within the cost centre or to move the service to a new cost centre and/or owner. In the event of the service being moved to a new cost centre, the stated approval process and policy will be invoked.

5.11 Separating employees

Separating employees must ensure that the device is returned to their respective manager, prior to the last day of employment and then returned to Health ICT.

5.12 Device disposal

A device may be disposed of in line with NSW Ministry of Health Policy Directive - PD2019_028 Goods and Services Procurement Policy.

5.13 Mobile Device Security, Care and Use

- Auto-lock, pin code or equivalent must be enforced on all of SESLHD ICT managed and user provided smart devices. This provides hardware level encryption and protects the information from privacy or confidentiality compromise if the device is lost or stolen.
- Removable storage devices such as Solid State Drives (SSD), USBs, SD cards or other such storage devices used in conjunction with a mobile service must be antivirus scanned and must have encryption enabled
- SESLHD takes no responsibility for any personal, or non SESLHD owned information or data that is stored on these devices that may be lost or deleted
- All backups of smart devices must be encrypted to ensure privacy and confidentiality of the backed up information
- Mobile devices operating systems need to be genuine, licensed and up to date. Devices or operating systems must not be tampered with to circumvent security, policy and configuration controls that have been enforced. Any tampering such as "jail-breaking" or "enabling privileged access" is strictly forbidden
- When not being used Wi-Fi and Bluetooth must be turned off to prevent discovery by third parties. All Bluetooth communications should use a unique passcode. It is not recommended to connect to unsecured Wi-Fi access points, if in doubt, do not connect
- Devices must auto lock after two minutes, or less
- User must not accept untrusted certificates from websites which will enable insecure browsing
- Users with voice only services connecting to external Wi-Fi access points take full responsibility of ensuring the devices operating systems are up to date
- Devices must be kept in a secure location

- Employees must take precautions to ensure data integrity and confidential information is not compromised. Including usage of non-SESLHD email facilities (i.e, Hotmail, Yahoo, Gmail) or other external resources to conduct SESLHD business
- Security breaches must be escalated to the employee's line manager and the SWSD to investigate immediately. Remediation steps may be appropriate including cancelling the service and wiping the device
- Tethering and personal hot spot functionality should be used in accordance with NSW Health acceptable use policies. Users should be aware that mobile data charges can be excessive when using these features and must take due care.

5.14 Compliance

Periodic audits will be conducted by ICT.

Monitoring the usage of the service including reviewing approvals, usage disclosure and compliance of NSW Health policies. This includes exception reports detailing usage patterns reflecting monthly call volumes and data usage. Where usage exceeds the allocation in three consecutive months, ICT will contact the cost centre owner and suggest options to reduce overspend/usage risk in line with the pricing structure as set under the Procure IT Framework with NSW Health. Health ICT reserves the right to audit the usage of SESLHD owned mobile phones without the employees consent, this includes excessive usage, inappropriate usage, unused services, devices containing SIM cards such as VPN sim cards. In the case of excessive or evidence of no usage over a period of three months the mobile services may be cancelled.

If evidence of non-compliance and continued disregard of this policy is determined, the Workforce Services Team will be engaged and consideration will be given for appropriate action including, removing the device from the employee and suspending the service.

5.15 Billing

Mobile telephone invoices are cross charged to each cost centre by Health ICT via monthly journal or invoices. These charges will include any courier costs on distribution of phone hardware, repair costs, balance of contract charges in the case of lost phones and usage charges.

5.16 Personal use of mobile devices (private usage)

SESLHD requires that personal usage that is any unrelated to an area/hospital/service business (private phone calls or data usage) be reimbursed to the district.
Pool phones are not included as private usage does not apply to these numbers.

The guidelines for personal use contained in the NSW Ministry of Health Policy Directive - PD2009_076 Use & Management of Misuse of NSW Health Communication Systems) applies equally to all types of devices.

Employees are responsible for notifying the Mobile Service Co-ordinator if they no longer require private usage on the device or they no longer have the device. Such notification must be certified by the cost centre or line manager. It is possible for an employee to make a notification and cancel contributions without relinquishing use of the service. A private phone call made by an employee to a family member, notifying that they are delayed because of employment related duties, is exempt from reimbursement.

Private usage contributions for staff, including Staff Specialists, are processed through payroll deductions.

Private Usage Amount

Estimated Usage	Usage Per Week	Per Week	Per Pay
None	0 minutes	NIL	NIL
Low	20 to 60 minutes	$4.00	$8.00
Medium	61 to 180 minutes	$7.00	$14.00
High	> 180 minutes	$10.00	$20.00

5.17 Cost Centre Manager Responsibility

Each cost centre manager is responsible for reviewing charges and usage of mobile phones allocated to their cost centre.

6. REFERENCES

- NSW Ministry of Health Policy Directive - PD2009_076 Use & Management of Misuse of NSW Health Communication Systems)
- NSW Ministry of Health Policy Directive - PD2019_028 Goods and Services Procurement Policy

7. REVISION & APPROVAL HISTORY

Date	Revision No.	Author and Approval
June 2018	0	Updated from previous PD 071 Mobile Phone Policy
August 2018	0.1	Updates – Linda Nguyen
April 2019	0.2	Updates from Executive Team and HR – Flora Karanfilovski
May 2019	0.3	Updates – Linda Nguyen
May 2019	0.4	Updates – Flora Karanfilovski & Linda Nguyen
May 2019	DRAFT	Draft for comment period
June 2019	1	Final version approved by the Executive Sponsor
July 2019	1	Formatted by Executive Services prior to tabling at August 2019 Executive Council meeting for approval to publish
August 2019	1	Approved at August 2019 Executive Council meeting to publish