ACT Health
Procedure
Mobile Communication Devices Management and Use

Contents

Purpose

To clearly outline the procedures associated with the management, use and administration of:

- Corporate mobile Communication Devices including SIM cards owned by the ACT Government; and
- Personal mobile Communication Devices including SIM cards for the purpose of gaining access to ACT Government Information and Communication Technology (ICT) resources and services, such as the Mobile Remote Email Service

Back to Table of Contents

Scope

This procedure applies to all Health Directorate employees, visiting health professionals, contractors, volunteers and any other people or corporate entities who use a mobile communication device and/or a SIM card for Government business or manage staff who use a mobile communication device and/or SIM card for Government business.

For the purpose of this procedure:

- Mobile communication devices include: mobile telephones, smart phones, iPads, iPhones, tablet computers, global positioning service (GPS) devices, small handheld devices, and any other device that can operate as a telecommunication or wireless mobile device.
- A SIM card is a smart card that stores data for mobile phone (GSM cellular) service providers and subscribers. SIM cards contain information that associate it to a specific service provider, and relevant data about the user of the mobile communication device such as user identity, location and phone number.
- Pagers are not considered to be a mobile communication device, as they only receive communication and cannot transmit information.
- Laptop computers are not considered under this policy and procedure. Use of laptop computers should follow *the ACT Government use of ICT Resources Policy.*

Except where stated otherwise all sections of this document apply to both to Government-owned mobile communication devices as well as personally-owned devices and/or SIM card(s) which have been authorised to access ACT Government ICT resources and services by their Executive Director.

Back to Table of Contents

Section 1 – Rationale

Allocation of Government-owned mobile communication devices and SIM cards must have appropriate Executive authorisation, in line with the allocation principles within this document.

Information associated with Business Use of a mobile communication device must:

- only be used for the purpose for which it was intended;
- be transferred to an appropriate ACT Government clinical or administrative system or file (electronic or paper-based) at the earliest opportunity; and
- be managed in compliance with the *Health Records (Privacy and Access)* Act 1997, the *Territory Records* Act 2002, and the *Workplace Privacy* Act 2011.

Particular care must be taken to protect the privacy and security of all Clinical Information.

All use of mobile communication devices and associated SIM cards shall comply with this procedure and the:

- ACT Health Information and Communication Technology Resources – Acceptable Use Procedure
- *Whole of Government (*WhoG) *Acceptable use of Information and Communications Technology (ICT) Resources Policy*;
- *Whole of Government Mobile Devices* Policy.
- *ACT Government Mobile Device Management (MDM) Configuration and Management Standard*
- *ACT Government Encryption Policy*
- *Health Records (Privacy and Access)* Act 1997
- *ACT Government Social Media Policy*

Back to Table of Contents

Section 2 – Roles and Responsibilities

Managers will:

1. Inform staff and users of their responsibilities under the *Whole of Government Acceptable use of Information and Communications Technology (ICT) Resources Policy, Whole of Government Mobile Devices Policy* and the *ACT Health Information and Communication Technology Resources Acceptable Use Procedure.*
2. Be aware of and enforce the *ACT Government Mobile Device Management (MDM) Configuration and Management Standard*.
3. Inform staff and users of this procedure if they will use a mobile communication device and/or a SIM card for Government business.

4. Inform staff and users of their responsibilities concerning the appropriate behaviour of staff under section 9 of the *Public Sector Management Act* 1994-34 and the ACT Government ACT Health Code of Conduct.
5. Notify the appropriate Manager or Executive Director of any suspected or alleged breaches involving non-compliance with the WhoG *Acceptable use of Information and Communications Technology (ICT) Resources Policy* and this procedure.
6. Allocate mobile communication devices based on the principles outlined in this procedure
7. To cater for such outages in mobile communication networks, business areas must assess the potential impact of an outage and develop a contingency plan to manage continuity of service.

Staff and Users will:

1. Be aware of and follow the requirements under this procedure, including the rules around applications on the mobile device.
2. Requests for mobile communication devices and/or a SIM card must be authorised by the Executive Director who is responsible for the relevant cost centre (or by the Deputy Director-General, or Director-General where the request is for an Executive Director or Deputy Director-General respectively).
3. Be aware of the requirements under the WhoG *Acceptable use of Information and Communications Technology (ICT) Resources Policy, Whole of Government Mobile Devices Policy* and the *ACT Health Information and Communication Technology Resources Acceptable Use Procedure* and follow those requirements.
4. Officers must sign the *Agreement for use of Corporate and Private Portable Electronic Devices*.
5. Ensure they have MDM installed on their mobile device used for Government business and be aware of the *ACT Government Mobile Device Management (MDM) Configuration and Management Standard*.
6. Be aware of the data available on their mobile device and ensure it is managed and stored as outlined in the procedure and shared only in accordance to the *WhoG Acceptable Use of ICT Resources Policy* and *ACT Health Information and Communcaiton Technology Resources Acceptable Use Procedure*.
7. Ensure that any loss or theft of Government devices is reported to Shared Services ICT (SSICT) as soon as possible.
8. Ensure that any requirement to cancel, transfer or dispose of Government mobile device must be reported to SSICT.
9. Mobile communication devices are issued to an Officer for the exclusive use of that person and must not be loaned to, or used by, any other person. Where a device has been issued to a business unit or section, the device is only to be used by members of that section, including for leave cover.
10. Government-issued SIMs are only to be used in Government-owned mobile communication devices. Personally-owned SIMs are only to be used in personally-owned devices.
11. Social media is only to be used in accordance with the *ACT Government Social Media Policy*.

12. Officers must not use voice-activated software (such as Siri) for any Business Use of a mobile communication device.

Back to Table of Contents

Section 3 – Allocation and Authorisation

All requests for mobile communication devices and associated SIM cards must be based on a valid business need and purchased through SSICT, unless otherwise authorised by the ACT Health Chief Information Officer (CIO). All telecommunication services will be provided by the telecommunication service provider contracted by ACT Government. Contracts with other service providers are not permitted for Government-owned mobile communication devices, unless a Business Case is provided to justify variation to the Whole of Government contractual arrangements (The Business Case requires Executive Director approval, and approval by the ACT Health CIO).

Allocation Principles:

a. Allocation is based on genuine business need – it is not based on an individual's position or role;
b. There is no intention of a non-salary financial benefit to the staff member;
c. Lower cost options should be considered. These may include pagers, voicemail, cordless telephones, pooling or reallocation of existing mobile communication devices;
d. The lowest cost option suitable for the task must be selected unless a specific business requirement exists for an alternate model;
e. An Officer should not be supplied with multiple mobile communication devices, unless there is a genuine business need, which is justified by the financial delegate;
f. Redeployment of existing mobile communication devices should be considered, prior to allocation of a new device;
g. Where a medical officer receives a mobile phone expense allowance in accordance with the *ACT Public Service Medical Practitioners Enterprise Agreement 2013-2017*, as amended from time to time, the medical practitioner cannot also be issued with a Government-owned mobile phone. However, use of shared mobile communication devices whilst on duty is permitted (e.g. use of wireless Voice Over Internet Protocol (VoIP) phone or tablet computer).

Back to Table of Contents

Section 4 – Mobile Device Management (MDM)

MDM is a software application or hardware appliance that implements policies for use of smart devices within the ACT Government. ACT Government implements Mobile Device Management (MDM) as part of any deployment or use of smart devices.

The MDM will define the security configuration of any device connecting to the ACT Government network, including but not limited to:

a. password policy (for example password length, device wiping after incorrect entry attempts);
b. screen timeout/lockout;
c. application control.

Specific configuration of these settings is defined for each compatible device platform in the *ACT Government Mobile Device Management (MDM) Configuration and Management Standard*.

Subject to written approval by authorised Health Directorate management, staff and other bodies will be empowered to self-register for access to information resources. Such registration immediately binds the individual to the rules and regulations applying to the access to Government information and the associated Laws of the Crown where applicable.

Officers must sign the *Agreement for use of Corporate and Private Portable Electronic Devices*, which includes reference to the use of geo-tracking.

All agreement forms (electronic or hardcopies) must be completed and signed prior to any access being granted. This includes personally owned devices.

Officers should note that corporate and personal mobile communication devices and/or SIM cards may be subject to Discovery or Subpoena and therefore may be required to be presented as evidence in a court of law. If the device is required for legal proceedings, anything contained on the device may be used as evidence, regardless of whether it is associated with business or private use of the device.

The ACT Government does not accept any liability for damage to personal smart devices and/or the loss/damage to data/applications caused by the connection to the ACT Government ICT resources.

Back to Table of Contents

Section 5 – Use of Mobile Devices

The user, having agreed to the conditions for the use of a personal device to connect to ACT Government ICT resources, is bound by all the conditions of use and policies associated with ICT use within the ACT Government.

Mobile communication devices which are obtained through the Private Practice Fund (PPF) will be considered to be personal mobile communication devices

The user having agreed to the conditions for the use of a corporate device to connect to ACT Government ICT resources is bound by all the conditions of use and policies associated with ICT use within the ACT Government.

Mobile communication devices are issued to an Officer for the exclusive use of that person and must not be loaned to, or used by, any other person. Where a device has been issued to a business unit or section, the device is only to be used by members of that section, including for leave cover.

The private and corporate use of a mobile device and or SIM card which has been used to connect to ACT Government ICT resources must be in accordance with the *ACT Government's Acceptable Use of ICT Resources Policy*.

All documents, photographs, videos, audio recordings and other files associated with the administrative and clinical use of the device will be:

- Stored with appropriate protection, in alignment with the relevant information classification, and in accordance with the *ACT Government Encryption Policy*;
- Managed in accordance with the *Clinical Records Management Procedure*;
- For photographs, video and audio recordings, they must be obtained with the consent of all parties (including, but not limited to the consumer, staff members and supervisor), (refer to *CHHS Photos, Video and Audio: Capture, Storage, Disposal and Use Procedure*); and
- Used only for the purpose for which they were collected, in accordance with the *Health Records (Privacy and Access)* Act 1997, *Territory Records Act* 2002, and the *Workplace Privacy Act* 2011

Back to Table of Contents

Section 6 – Applications

The only approved applications to be installed and operated on these devices are those that have been acquired through the mobile operating system vendor's official application store or made available by the ACT Government application store, which is accessible through the MDM software application. Users must not install any application on the MDM application blacklist, or must remove these upon notification by the MDM of non-compliance with the *ACT Government Mobile Device Management (MDM) Configuration and Management Standard*.

The ACT Government also reserves the right to require that additional software is installed and activated to grant or retain access to corporate resources. An example of when this may occur would be installation of an anti-malware application to mitigate risks on a specific device platform. Notification on non-compliance of blacklisted or required applications will be either automatically sent via email by the MDM, or manually by the MDM system administrators after a compliance audit.

Applications that are used to consume corporate information, like word processors, spreadsheets and PDF or power point readers need to be configured to protect corporate information. Many of these applications provide integration with unapproved cloud based services that must not be used with any corporate information that is not public domain. Where such applications include additional encryption like 'Data Protection' support, this needs to be enabled to provide additional protection to corporate information. Where applications open an unsanctioned web service to share or provide an out-of-band method of transferring information, this functionality must not be used for work related purposes. Staff should be aware that the MDM will scan the user's device for malicious apps, and will therefore require access to the full app inventory list from the device.

Back to Table of Contents

Section 7 – Compliance

The device must only be used by the authorised user(s). It is the sole responsibility of the authorised user(s) to ensure that the device is used in a manner compliant with this procedure. If it is determined that anyone using the device has breached this procedure, the authorised user(s) will be held accountable and will be deemed as having been non-compliant with this procedure.

Failure to comply with this procedure will be deemed a security violation and render any employee of the ACT Government subject to disciplinary action under the relevant Enterprise Agreement, and may include termination of employment, unless a waiver from compliance with an element of the procedure is sought and granted.

Failure of any agent of the ACT Government who is not an employee under the *ACT Public Service Act*, or any incorporated, or non-incorporated body accessing ICT resources on behalf of the ACT Government to comply with this procedure will be deemed a violation of security. A breach of contract and damages will be sought to the limit as specified in the contract, and possible termination of contract, unless a waiver from compliance with an element of the policy is sought and granted.

If a Business Unit believes that they have a good reason for not complying with this procedure, they should follow the procedure set out in the *Policy Waiver Procedure* by contacting the ACT Health Chief Information Officer.

Back to Table of Contents

Section 8 – Jail breaking / Rooting

Jail breaking or rooting of a device which involves deliberate interference with the device and/or SIM card security controls, will be deemed a violation of this procedure. Any device found to be jail broken or rooted will be wiped with or without the user being notified. If the

device is privately owned, then the device will be blocked from connecting to ACT Government ICT resources. Disciplinary action may also be undertaken against the authorised user of the device regardless of whether this is a personal or corporate device.

Back to Table of Contents

Section 9 – Data Storage

Email, calendar and contact information is to be stored with appropriate protection, in alignment with the information classification and in accordance with the *ACT Government Encryption Policy*. This also applies where other types of data are exposed to a smart device, for example access to ACT Government file systems, SharePoint or other intranet services via a secure terminal or VPN connection.

Applications and data are to be stored on the device with the protection features of the device and in accordance with the *ACT Government Encryption Policy*.

Personal applications and data are not to interact with the corporate or ACT Government installed applications e.g. corporate data, email and/or email attachment shall not be copied to a private email or data sharing application and sent. Users shall not use unapproved public cloud based services via a web browser or applications to transmit or store corporate data. Existing approved externally hosted applications used by directorates may be used where there is a secure channel to the service (for example SSL protected web portal).

Connection to data stores will be by Citrix or approved equivalent software (for example Acronis Access). Access may also be available using a secure connection via the security software inherent in the phone and MDM for providing a safe connection. This is only available after approval has been obtained from the relevant business owner.

Back to Table of Contents

Section 10 – Data Security

Classified and sensitive information must not be stored on a mobile communication device, unless the device has been specifically approved for this purpose by the Health Directorate, in conjunction with SSICT Security Team. Where storage of such data is authorised, all available protection mechanisms must be used to protect the information. In addition, a copy of the information should be transferred to an appropriate ACT Government clinical or administrative system or file as soon as possible, and then removed from the device once it is no longer required. Officers may contact the SSICT Service Desk for assistance, if required (ph: 6207 9000).

Work-related information must be used only for the purpose for which it was intended and use of this information must comply with the *Health Records (Privacy and Access) Act* 1997,

Territory Records Act 2002, and the *Workplace Privacy Act* 2011. In keeping with this legislation, official records must be created in relation to business use of the device, and stored in an appropriate ACT Government system or Official File (this may include transcription of SMS or telephone conversations, in addition to other information captured on the device).

Access to ACT Government data is to be via approved avenues only (such as ACT Government fixed or wireless networks, Citrix, OWA, or the iOS Remote E-mail Service).

Synchronisation of mobile communication devices with ACT Government computing equipment may only take place with approval from SSICT. Officers should note that whilst a device may have the capability to be synchronised, this does not automatically mean that synchronisation is authorised by SSICT.

Except where a Health Directorate approved process exists, no information is to be exchanged between a mobile communication device and a device which is intended for medical purposes (or associated software). Approval may only be granted in line with the ACT Health Chief Information Officer and SSICT Security requirements.

Officers must not use voice-activated software (such as Siri) for any Business Use of a mobile communication device.

- SSICT has obtained the following advice from Apple in relation to Siri: “the things you dictate will be recorded and sent to Apple to convert what you say into text. Your device will also send Apple other info, such as your first name, nickname; the names, nicknames, and relationship with you (e.g. dad) of your address book contacts; and song names in your collection”.
- Officers are not permitted to use Siri for dictation, for reading or composing e-mails, or for any other purpose related to Business Use of a mobile communication device.
- Other voice-activated software should not be used unless approval has been provided by the SSICT Security Team and the Health Directorate.
- In order to protect the confidentiality of ACT Government data, SSICT assesses software to determine potential security risks associated with use of that software. In the case of voice-activated software, this assessment includes determining whether the software operates in a standalone capacity or potentially sends the transcribed information to an external party or cloud based service. Applications such as Siri, and some other dictation products, currently do not meet ACT Government security requirements. On request, the SSICT Security Team will assess other voice-activated software to determine whether it is suitable for use within the ACT Government.

Back to Table of Contents

Section 11 – Security and monitoring

The physical safety and security of the device is the responsibility of the Officer, who must take all precautions to safeguard the mobile communication device. All mobile communication devices must be protected through use of a PIN, security pass code, fingerprint or facial recognition if available on the device.

SSICT will monitor and maintain logs of mobile communication devices connected to the Mobile Remote Email Service, and ACT Government fixed and wireless networks. This may include auditing of every device, whether Government-owned or personally-owned. This will include details of use, applications (apps) installed, and geographical location.

Unauthorised access and inappropriate use of mobile communication devices will be reported by SSICT whenever it is detected. Supervisors are responsible for advising Officers to become familiar with their responsibilities in relation to the *Acceptable Use of ICT Resources Policy*, the *ACT Government Smart Device Security Policy*, and the *Whole of Government Mobile Devices Policy*.

Where deemed necessary by the Health Directorate Internal Audit and Risk Manager, audits of mobile communication device records may be undertaken as part of the Health Directorate Internal Audit process.

If you believe your device has been compromised or tampered with in any way, you must contact the ICT Service Desk for assistance and advice (6207 9000) as soon as possible.

Back to Table of Contents

Section 12 – Back up of data

Where clinical or administrative information is captured or stored on a mobile communication device, the Officer must transfer a copy of this information to an appropriate ACT Government clinical or administrative system or file as soon as possible. Once the information is no longer required, it should be deleted from the device, so long as it has first been transferred to an appropriate ACT Government system or file. The Officer should undertake regular checks of the device to make sure information is only retained on the device for as long as necessary.

Where it is necessary for a delay in the process of transferring information to an appropriate ACT Government clinical or administrative system, the Officer must make sure that information is backed up, to protect against loss of information and breach of record-keeping legislation. Backups of information stored on a mobile communication device, which has been approved for business use, must be encrypted and protected by a password which complies with the *ACT Government Password Policy and Standard*.

Backups of personal devices must be encrypted and protected by a password which complies with the *ACT Government Password Policy and Standard*. Wherever possible, backups should be stored on ACT Government ICT resources. Backups must not be made or stored on a public computer, or externally hosted storage services including cloud based services (except where use of specific storage services are explicitly authorised by SSICT Security). Use of ACT Government storage solutions is permitted.

For assistance with selecting and installing approved backup software appropriate for the specific mobile communication device, the Officer should contact the SSICT Service Desk (6207 9000).

Prior to repairs or maintenance being undertaken, all business data must be transferred to an appropriate ACT Government system or file (except where damage to the device prevents this). Once it has been transferred to an appropriate ACT Government system or file, all data must be removed from the device.

Back to Table of Contents

Section 13 – Contingency Planning

Networks which enable mobile communication devices to operate (such as commercial mobile phone networks and wireless computing networks) may experience periods of downtime, whether planned or unexpected.

To cater for such outages in mobile communication networks, business areas must assess the potential impact of an outage and develop a contingency plan to manage continuity of service. This is particularly relevant for areas that provide clinical services or business critical services through a mobile phone service.

Back to Table of Contents

Section 14 – Wiping

For a Corporate Device, wiping of the device will be undertaken with or without the user being notified:

a. if a breach of this procedure has been determined
b. if the device has been reported lost or stolen
c. before disposal of the device
d. of selective wiping prior to the device no longer being required to connect to ACT Government ICT resources

For a Personal Device wiping of the device will be via a selective wipe where possible. Wiping and permanent removal from the ACT Government MDM may be undertaken depending on

the circumstances. Full device wiping for personally owned devices would normally only occur with the consent of the owner if deemed a requirement to prevent harm to the ACT Government's information or systems.

Back to Table of Contents

Section 15 – Workplace Privacy

The use of a smart device must maintain workplace privacy in accordance with the *Workplace Privacy Act (2011)*. Geo-tracking is normally enabled on these devices. It is recommended that this feature is disabled wherever possible when determining geo-location is not required for work purposes. Users of corporate owned devices are responsible for the management of files generated by the GPS and other geo-tracking function. Any geo-tracking files discovered as part of a duly authorised investigation may form part of the investigations evidence.

Back to Table of Contents

Section 16 – Connectivity

Connections to ACT Government networks will be limited to defined approved channels - for example wireless from the Internet (4G or wireless) to MDM, or the use of an official ACT Government wireless network.

Alternative connections must not be used and will be considered a breach of this procedure, these include:

a. a wired network (LAN) connection to ACT Government networks
b. Bluetooth to an ACT Government workstation

The use of wireless connections on untrusted networks (such as WiFi hotspots at hotels, cafes and airports) should be undertaken with great care due to the increased exposure to information theft and device compromise on such networks. Physical and information security are of paramount importance when travelling abroad.

Bluetooth access must only be used for the following purposes:

a. connection of a Bluetooth headset/in car device
b. tethering for internet access.

Staff should ensure that they receive a trusted certificate when attempting to access secure resources. This will be indicated in the browser address bar and depending on the type and version of the browser in use, staff may be prompted to choose to connect or not.

Back to Table of Contents

Section 17 – Device Firmware

Corporate and personal devices must have firmware no older than the previous version to the latest or most current firmware version available.

SSICT will (as part of the MDM) implement monitoring and logging which will make users aware of necessary patches and firmware updates. Users will be granted 28 days to install the updates after which time the device will become non-compliant with the MDM posture assessment and may be prevented from accessing corporate resources until brought into conformance, dependant on estimated risk to the ACT Government. Exceptions may be granted if technical issues prevent firmware updates. Such exemptions will require SSICT Security approval and be documented in Service Now until resolution of the technical issue/s is achieved.

Back to Table of Contents

Section 18 – Out of band security updates

The SSICT Security team may vet a mobile device update as being highly critical and subject to an immediate update that may occur outside of normal business hours. The terms of the update will be managed via the existing change control processes regarding emergency changes. This may bring a requirement for updates to be applied in a more immediate time frame.

Back to Table of Contents

Section 19 – Costs associated with Mobile Communication Devices

For Corporate Devices, the person who authorises the request (i.e. Executive Director, Deputy Director-General, or Director-General, as appropriate) is responsible for making sure costs associated with the device are budgeted for within the business area, managed appropriately and that services associated with the device are cancelled once no longer required. The business area may seek reimbursement of costs from an Officer relating to their private use in excess of agreed amounts.

Where access to the Mobile Remote Email Access Service is authorised for personally-owned devices, the business area is responsible for the annual service fee, however all other costs are to be borne by the Officer who has applied to use their personally-owned device. The Authorising Officer must advise the Officer of potential cost implications. Officers should be aware that use of their personally-owned device to access ACT Government networks or services (including the Mobile Remote Email Service) will likely result in increased data utilisation. It is the Officer's responsibility to make sure they have an adequate data plan in place; and costs associated with the data plan are the responsibility of the Officer

The following outlines the procedure for reimbursement of charges:

- Where an Officer is provided with a Government-owned (corporate) mobile communication device, the Officer is responsible for reviewing bills associated with the device and identifying private use where relevant (for example use of the device while overseas)
- The Officer agrees to reimburse the Health Directorate for excessive or unreasonable charges relating to private use, including costs associated with international roaming not previously approved, or costs to numbers not covered by the mobile plan such as 1300 numbers or numbers associated with non-standard charging rates.
- Where private use exceeds reasonable use, the Officer will reimburse the Health Directorate for charges associated with private use of a Government-owned (corporate) device. Reimbursement of charges can be progressed through Attachment A – Banking Advice Slip, Reimbursement for Private Use of a Health Directorate Mobile Communication Device.

The following outlines the procedure for international roaming:

- Use of mobile data when overseas can have significant cost impacts. For Government-owned devices, an Officer must apply for international roaming prior to each overseas trip and the Officer's financial delegate must agree to pay international roaming costs. The Officer will be required to reimburse the Health Directorate for costs relating to private use of the device.

The following outlines the procedure for centralised billing:

- Digital Solutions Division, will maintain a database of Government-owned mobile communication devices for the Health Directorate. This database will be used to enable the automated billing process, and may be accessed for audit purposes.
- All costs associated with mobile communication devices and/or SIM cards are the responsibility of the allocated business unit, as per the Cost Centre and financial delegate information provided.
- An automated process will be used to allocate invoiced costs for Health Directorate mobile communication devices and/or SIM cards. This process will assign costs to the Cost Centre identified for each mobile communication device and/or SIM card
- Each business unit is responsible for identification of any billing errors. Where a billing error is identified, the business unit will provide written notification through SSICT, who will action as appropriate.
- Where a variation to the allocation, Cost Centre or financial delegate is required, the business area is responsible for notifying SSICT Service Desk accordingly. The business area will be responsible for costs associated with the device until such time as this written notification of changes is provided to SSICT.
- The financial delegate is responsible for confirming that services associated with mobile communication devices (such as data plans) are cancelled once no longer required, as services may be renewed automatically by the service provider, in which case charges

will continue indefinitely, until a written cancellation request is provided. Cancellations cannot be backdated.

Back to Table of Contents

Section 20 – Repairs and maintenance

Devices such as mobile phones are purchased outright through SSICT.

Some repairs may be covered by the device warranty, while some may incur charges. The financial delegate is responsible for assessing quotes for charges in consultation with SSICT to determine an appropriate course of action. This may include requiring the Officer to fund the repairs where they were at fault, covering future repairs with insurance such as Apple Care, or covering the repairs from the business area's budget.

Where possible, prior to repairs and maintenance being undertaken, all business data must be transferred to an appropriate ACT Government system or file to prevent loss of data and unauthorised access to information (except where this is not possible due to damage to the device). Where possible, once it has been transferred to an appropriate ACT Government system or file, all data must be removed from the device prior to providing to an external repairer (for assistance, contact the SSICT Service Desk (6207 9000).

Repairs must be performed by an authorised repairer unless approval by the Chief Information Officer has been granted to use an alternative repairer.

SSICT cannot guarantee that a device which is sent for repairs and maintenance will be returned. In some cases a replacement device may be supplied by the repairer.

Back to Table of Contents

Section 21 – Loss or theft

If a government mobile communication device is lost or stolen, you must notify SSICT Service Desk without delay to suspend (not cancel) the mobile phone number– telephone (02) 6207 9000. The SSICT Service Desk can suspend access to ACT Government networks and services, including the Mobile Remote Email Service, and in addition, for certain devices, it may be possible to locate the device, using location services.

Where the lost or stolen device is privately owned and (authorised to access ACT Government ICT resources and service), SSICT must be notified immediately. The SSICT Service Desk can suspend your access to ACT Government networks and services, including the Mobile Remote Email Service.

You must also notify your Supervisor and provide details of actions taken (such as requesting suspension/cancellation of service).

It is the responsibility of the user to ensure that as soon as possible after the detection of a theft or loss of a device, that the device is wiped. A self-service portal is available on the MDM to allow device users to wipe their own devices. If there is an issue with this process SSICT will need to be engaged to assist.

In instances where the mobile service has been suspended, the suspension must be reviewed by the program after two weeks to decide if the service should be cancelled as suspended services still continue to bill. Typically, if the device is not located within 2 weeks, the service should be either re-allocated to a new SIM card re-issued to a new device or cancelled.

In the event that the device is subsequently located, the suspension can be lifted and the service reactivated by SSICT.

Replacement of any lost or stolen device is at the discretion of the financial delegate, who will be required to pay for the replacement device, and any costs associated with cancellation of the lost or stolen device.

Back to Table of Contents

Section 22 – Disposal or Transfer/Redeployment

The physical device is purchased outright by the area, facilitated through SSICT. SIM cards and services associated with the device have recurrent expenses. A Government-owned mobile communication device and associated SIM must be returned if the Officer leaves the organisation, or no longer requires use of the device unless appropriate approval is otherwise provided.

If an officer transfers to another section of the organisation and retains their device and SIM, the financial delegate must advise SSICT and provide the details of the Cost Centres involved in the transfer of the device and SIM. This will allow SSICT to transfer the monthly cost associated with the mobile Communication device and SIM.

If an Officer transfers to another ACT Government Directorate, the Health Directorate delegate may choose to make arrangements with the other agency to enable transfer of the Government-owned SIM or device through SSICT.

Supervisors are responsible for confirming that mobile communication device and SIM, and all associated accessories are returned.

The physical device can be reallocated, returned or disposed as per service requirements. Disposal of hardware should be coordinated through the Digital Solutions Division. However, there are no refunds associated with this transaction.

The SIM card associated with the device (if any) can be re-allocated or disposed. The reallocation or disposal of a SIM must be coordinated through SSICT.

Prior to disposal of a device the user is to ensure that the device has been completely wiped and reset to factory default settings.

If the device is an Apple device, it is important that the Officer has logged the device out of the user's iTunes accounts and links to personal iTunes accounts removed. If this does not occur, the device cannot be redeployed.

Staff with corporate devices protected by activation locks (for example iCloud) provided by the operating system are required to remove these anti-theft activation locks prior to returning to the ACT Government.

If a Corporate Device is no longer required to connect to ACT Government resources then a complete wipe of the device is to be undertaken prior to the access to ACT Government ICT resources being removed for the device.

If a Private Device is no longer required to connect to ACT Government resources then a selective wipe (where practicable) or complete wipe of the device is to be undertaken prior to the access to ACT Government ICT resources being removed for the device.

When an Officer leaves the organisation, the Health Directorate will not permit the Officer to retain a Government-supplied SIM or device, unless the application is authorised by the appropriate financial delegate (Executive Director, Deputy Director-General, or the Director-General, as appropriate).

Arrangements in relation to reimbursement for a mobile communication device and any accessories, will be based on a device life expectancy of 24 months, or the duration of the lease (whichever is greater).

For example: if a mobile telephone with a life expectancy of two years cost $1,000, an Officer who is authorised to take the device with them one year after it was purchased is required to pay a pro-rata amount for the device of $500 (i.e. half the original purchase price, as half the device life is remaining). The Officer must also pay the pro-rata amount for all associated accessories.

The Officer must coordinate the release of the SIM card with SSICT. Where the departing Officer fails to provide appropriate details for the transfer prior to their separation date, all services associated with the device will be cancelled.

Officers must wipe all personal data from the device prior to returning it. Advice should be sought from the SSICT Service Desk in relation to wiping processes.

Where a mobile communication device is returned by an Officer, the financial delegate may authorise the redeployment of the device. However, the financial delegate must coordinate changes through SSICT regarding the reallocation of the SIM and provide updated details so that Health Directorate records are kept up to date. In addition, prior to redeploying the device, care should be taken to make sure that any data contained on the device has been transferred to an appropriate ACT Government clinical or administrative system or file, and subsequently removed from the device.

If the financial delegate does not wish to redeploy the mobile communication device, it must be returned to the Digital Solutions Division, together will all accessories and security information specific to the device.

A staff member who transfers from another area of the ACT Government may bring their Government-owned mobile communication device with them, so long as they have obtained approval of the appropriate Health Directorate financial delegate (Executive Director, Deputy Director-General, or Director-General, as appropriate) who will be responsible for costs associated with the device. Transfers must be coordinated through SSICT, who will facilitate the transfer and maintain appropriate records for the device.

Once a transfer has been agreed to, the Government-owned mobile communication device will be managed as if it had been originally purchased by the Health Directorate.

Back to Table of Contents

Section 23 – Cancellation of service / opt-out provision

Where an Officer, supervisor, business unit, or section wishes to cancel services associated with a Government-owned mobile communication device, the financial delegate for the affected area will be responsible for the payment of any penalties that may be incurred for early cancellation.

It is the responsibility of the financial delegate to inform SSICT that the device is no longer being used to enable cessation of monthly charges.

Where an Officer has elected to use their personally-owned device to connect to ACT Government networks and services, the Officer may choose to 'opt-out' of the service at any time; however:

- The Officer must notify SSICT;
- The Officer must erase all corporate data from the device (having first transferred the data to an appropriate ACT Government file or system). Advice should be sought from SSICT in relation to wiping processes; and

- Supervisors are responsible for advising Officers to note their obligations in this regard, and monitoring compliance with this provision.

Back to Table of Contents

Implementation

Staff will be referred to this Procedure when they apply to conduct Government Business on their device.

Back to Table of Contents

Evaluation

Outcome Measures

- All access requests for Mobile Communication Devices are authorised by the appropriate Executive Director (or a Deputy Director-General or the Director-General, as appropriate), without this approval Mobile Communication Devices or SIM will not be provided through SSICT.
- All access requests for iPhones and iPads are accompanied by a signed *Agreement for Use of Corporate and Private Portable Electronic Devices,* this is a requirement for SSICT to process the request.

Method

- Shared Services ICT to report the number of licenced and authorised users to the ACT Health CIO on an annual basis.

Back to Table of Contents

Related Policies, Procedures, Guidelines and Legislation

Policies

- ACT Health Information and Communication Technology Resources – Acceptable Use
- CHHS Clinical Records Management Policy
- WhoG Acceptable use of Information and Communications Technology (ICT) Resources Policy ACT Government Smart Device Security Policy
- Whole of Government Mobile Devices Policy
- ACT Protective Security Policy Framework
- ACT Government ICT Security Policy
- ACT Government Password Policy and standards
- ACT Government Social Media Policy
- ACT Government Encryption Policy

Procedures

- CHHS Photos, Videos and Audio: Capture, Storage Disposal and Use Procedure

Guidelines

- ACT Government Purchasing Guide
- ACT Government Mobile Device Management (MDM) Configuration and Management Standard

Legislation

- *Health Records (Privacy and Access) Act* 1997
- *Human Rights Act* 2004
- *Work Health and Safety Act* 2011
- *Territory Records Act* 2002
- *Privacy Act* 1988
- *Workplace Privacy Act* 2011
- *Road Transport (Offences) Regulation* 2005
- *Spam Act* 2003
- *Public Sector Management Act* 1994

Back to Table of Contents

References

1. ACT Government Smart Devices Policy, Version 1.1, June 2017.
2. ACT Government Acceptable Use of ICT Resources Policy, Version 2.5, 23 January 2017.
3. Agreement for use of Corporate & Private Portable Electronic Devices (http://sharedservices/actgovt/ICTforms/Portable-Electronic-Devices-Agreement.doc)
4. ACT Government ICT Security Policy, Version 2.5, 14 July 2017.

Back to Table of Contents

Definition of Terms

Administrative use	Use of a mobile communication device in relation to activities normally associated with the administration of Government business.
Business use	Use of a mobile communication device for any purpose which is on behalf of, or for the benefit of, the ACT Government. Business use may include clinical use and administrative use.
Clinical use	Use of a mobile communication device in relation to the provision of treatment to a healthcare consumer.
Cloud based service	Data storage facilities accessed over a network using Web Services communication methods.
Corporate data	Information which relates to any Business Use of the mobile communication device, including any data which relates to the work of the ACT Government.

Geo-tracking	The ability to use location tracking services to identifying the physical location of a mobile communication device.
Corporate device	A smart device that is owned by the ACT Government, and provided to an individual for the conduct of Government business plus approved incidental private use.
International roaming	The ability to use a mobile telecommunication device to connect to a communication network (such as 4G) while overseas.
Email Service	A service which enables access to email resources (email, contacts & calendar) via smartphone or tablet.
iTunes	iTunes is an application developed by Apple Inc. that allows users to purchase and download applications, music, videos and books for use on a computer or other iTunes compatible device.
Jail Breaking	The deliberate act to remove the manufacturers controls on the device so as to load software or carry out acts that could prejudice the secure operation of the device.
Mobile communication device	A portable device which can be used for electronic communications. This includes mobile telephones, smart phones, iPads, iPhones, tablet computers, global positioning service (GPS) devices, small handheld devices, and any other device that can work as a telecommunication or wireless mobile device.
Mobile Device Management (MDM) Mobile Remote	A software application or hardware appliance that implements policies for use of smart devices within the ACT Government (including, but not limited to: password policy, screen time-out, and application control).
Officer	A Health Directorate employee, visiting health professional, contractor, volunteer or any other persons to whom this policy applies (refer Scope)
Personal device	A smart device that is not owned by the ACT Government, but is the personal property of the user or corporate entity but that is used for Government business.
PIN	Personal Identification Number – a security number required to gain access.
Private use	Private Use is using the device for any purpose that could not be construed as acting on behalf of or for the benefit of the ACT Government.
Rooting	A common term used on non-apple devices of gaining access to the control layer to subvert the manufacturer's controls on the device so as to load software or carry out acts that could prejudice the secure operation of the device.
Security pass code	A pass code required to gain access to a mobile communication device.
Selective Wiping	The deletion of an identified storage area on a device so that the information stored thereon is unrecoverable by normal use.
Shared Services ICT (SSICT)	ACT Government ICT service provider.
SIM – Subscriber Identity Module	A card issued by a telecommunications provider to enable identification of the user, and to facilitate access to services.
Spam	Spam is a generic term used to describe electronic 'junk mail' – unwanted messages sent to a person's email account or mobile phone.
Synchronisation	When a set of data or files are identically copied into another location.

VPN	VPN stands for Virtual Private Network and is used to connect remote users into the ACT Health network.
Wiping	the deletion of the entire contents of the mobile device to an unrecoverable level
Wireless Network	A computing network which is accessed using wireless networking infrastructure and protocols. Cables are not required to connect a computer to a wireless network.

Back to Table of Contents

Search Terms

Mobile devices, mobile communication, iPhone, Android, SIM, phone, ipad, tablet, communication, ICT, IT, remote, WiFi.

Back to Table of Contents

Attachments

Attachment 1 - Banking advice slip

Disclaimer: *This document has been developed by ACT Health specifically for its own use. Use of this document and any reliance on the information contained therein by any third party is at his or her own risk and Health Directorate assumes no responsibility whatsoever.*

Policy Team ONLY to complete the following:

Date Amended	*Section Amended*	*Divisional Approval*	*Final Approval*
July 2018	*New Procedure*	*Digital Solutions*	*Digital Solutions*

This document supersedes the following:

Document Number	*Document Name*
DGD13/002	*Mobile Communications Devices Requests SOP*
DGD13/002	*Mobile Communications Devices – Private use of Government owned devices Procedure*
DGD13/002	*Mobile Communications Devices Management and Use policy*

Attachment A – Banking Advice Slip

Reimbursement for Private Use of a Health Directorate Mobile Communication Device

Payments can be made at the Cashiers Office, ground floor, TCH; or the Dental Clinics within Civic, Belconnen, Tuggeranong and Phillip Health Centres.
This form must be completed for payments to be processed.

Note: 10% GST must be applied to payment of costs for private use of a Health Directorate mobile communication device; however, a Tax Invoice is not required.

Description of Goods or Service	Amount $ (Excl. GST)	Entity	Cost Centre	Account Code	Int. Trad.	Project	Agency Use	GST Tax Type
Repayment of costs associated with private use of a Health Directorate mobile communication device.		600		713216	99	99999	9999	10% AP
	Total $ (excl. GST)			**Total $ GST**		**Total Amount $ (inc. GST)**		

Signature of Payer		**Date**
Name of Payer (please print)		
Section and Division/Branch		
Signature of Cost Centre Delegate		**Date**
Name and Position Number of Cost Centre Delegate (please print)		
Section and Division/Branch		

Please attach any relevant documentation.
For audit purposes, Officers must maintain a record of identified private use, and repayments of costs, in consultation with the financial delegate.