

# DEDJTR Intranet

## Mobile telephones, smart phones and tablet devices policy

Version number	1.19
Policy owner/branch	Manager, Technology Services Division
Approved by	--
Creation date	20 February 2015
Last modified date	17 May 2017
Effective date	--
Review date	12 months after effective date
TRIM reference	DOC/17/241606

### Sections within this policy

1. [Scope](#)
2. [Policy statement](#)
3. [Principles](#)
4. [Allocation and devices](#)
  - 4.1 [Mobile/smart phones](#)
  - 4.2 [Tablet devices](#)
  - 4.3 [Asset management](#)
  - 4.4 [Temporary allocation of devices](#)
5. [Replacement of devices](#)
6. [Non-work use](#)
  - 6.1 [Internet, applications and social media](#)

- 6.2 [Privacy](#)
- 6.3 [Travel/roaming costs](#)
- 7. [Responsibilities](#)
  - 7.1 [DEDJTR people](#)
  - 7.2 [Line managers](#)
  - 7.3 [Business managers](#)
  - 7.4 [Technology Services Division](#)
  - 7.5 [Director](#)
- 8. [Security](#)
- 9. [Loss, theft or damage](#)
- 10. [Monitoring and reporting](#)
- 11. [Occupational health and safety](#)
- 12. [Breach of policy](#)
- 13. [Definitions](#)
- 14. [Related information](#)

## 1. Scope

This policy applies to all DEDJTR people who use a DEDJTR-owned mobile device. All devices containing a Subscriber Identity Module (SIM) are encompassed in this policy, including approved mobile telephones, high speed wireless modems, iPads, smart phones and networked appliances.

## 2. Policy statement

This policy is important in supporting a flexible workforce, connecting people to the people, tools and information needed, when and where they work. It aims to provide a balance between guidance on appropriate use, management of costs and assets and support for collaboration in a mobile workforce.

This policy outlines the approach to the purchase, allocation, management and use of mobile telephones, high speed wireless modems, iPads, iOS smart

phones and networked appliances in the Department of Economic Development, Jobs, Transport and Resources (DEDJTR).

### 3. Principles

- Mobile devices are issued where there is a demonstrated business requirement. The decision to allocate a mobile device rests with a director.
- People who, as a consequence of their role need to be in regular contact with others in the department or other stakeholders, or for reasons of isolation or personal safety may request a mobile device. In addition mobile devices may be requested where they support access to information and tools to support a mobile workforce.
- DEDJTR supplied devices are departmental assets and remain the property of the department while allocated. Devices must be returned to the Technology Services division upon cessation of employment.
- DEDJTR people are expected to reimburse the cost of making non-work voice calls and SMS/text messaging, where those costs exceed \$15 per month.
- DEDJTR allows private mobile/smart phones or services to access DEDJTR mail or applications (also known as 'Bring your own device' or BYOD) under certain conditions to ensure security. For more information, refer to the BYOD policy.

### 4. Allocation and devices

#### Allocation and devices

The decision to purchase or allocate a mobile device rests with a director.

Directors who approve the purchase of a mobile device:

- must be satisfied there is a demonstrated business need;
- must have an appropriate financial delegation and ensure there is sufficient ongoing budget capacity to cover purchase, usage and service costs.

All mobile devices and associated services must be purchased using the mobile device request form.

All DEDJTR-owned mobile devices must have the department's mobile device management software installed prior to allocation to DEDJTR people.

Selection of device will be aligned to specific demonstrated and identified business requirements. Currently, only Nokia phones, Apple smart phones and tablet devices are provided by the department.

## 4.1 Mobile/smart phones

Criteria demonstrating business need includes:

- the provision of a mobile device is required to perform work duties, or the provision of a mobile device would significantly improve the efficiency and effectiveness of work output.
- the person is frequently required to perform duties away from their usual work base, and needs to be contactable for urgent matters.
- the person regularly works alone out of the office and requires a level of security provided by use of a mobile device.
- there is a regular, ongoing need for the person to be contacted for work matters. This may include the need to be contacted outside of ordinary business hours.
- there is a regular, ongoing need for the person to access corporate applications, data collection applications, monitoring tools or social media outside of ordinary business hours or while travelling.

## 4.2 Tablet devices

Tablet devices are generally issued where the business requirement for features, such as corporate applications, monitoring tools, undertaking scientific research, or access to document annotation and editing capability are required, which cannot be easily accessed using a smart phone.

Consideration of the business need for a tablet device should include a review of the full suite of tools provided for business use. Opportunities to rationalise and/or consolidate other devices should be considered to control costs. For example, the provision of a tablet device may result in there no longer being the need for access via a desktop, laptop etc.

## 4.3 Asset management

All devices purchased by DEDJTR remain the property of the department when allocated to DEDJTR people.

It is the responsibility of the device holder to return the device to the Technology Services division for secure disposal or reallocation prior to leaving the department.

Mobile device holders may apply for approval to retain their device when they move between Victorian Government departments. The transfer must be approved and actioned by the Technology Services division.

In the case of transfer to another business unit or change of role within DEDJTR, the justification for allocation of a mobile device must be reviewed by the device holder's incoming business unit prior to the user transitioning into their new role. If the device is not required in the new position, the device must be returned to the Technology Services division.

In some circumstances, with the approval of their line manager, a DEDJTR person may be allowed to retain a **mobile phone number** when they leave the department, provided that there is no adverse business impact to DEDJTR.

The Technology Services division maintains a register of issued mobile devices.

## 4.4 Temporary allocation of devices

In some instances business units may require some staff to have access to mobile devices for short periods of time (for example, emergency response, on-call, off site, travel or short term initiatives over large or remote areas). In these cases, business units may maintain a pool of devices, to be allocated for short term use.

DEDJTR people must return any pool device allocated to them upon return to their regular work location or activity.

The business unit manager is responsible for:

- issue and retrieval of pool devices;
- maintaining a register of available and allocated devices;
- monitoring voice, text and data usage on a monthly basis and;
- secure storage of unallocated devices.

## 5. Replacement of devices

The replacement of a DEDJTR owned mobile device requires the approval of the appropriate director.

Device replacements will only be considered if the following criteria are satisfied:

- an ongoing demonstrated business requirement;
- the device is a minimum of two years old;
- the device has been lost, stolen or irreparably damaged.

Where possible, the department will replace lost, damaged or stolen devices with devices held in stock.

## 6. Non-work use

DEDJTR issued mobile phones and devices are provided for official work-related use. This includes use of a mobile device's camera facility, global positioning system and internet connectivity.

Departmental mobile devices must not be used for unlawful purposes or to solicit, advertise or in any other way, promote the conduct of a staff member's private business.

A limited amount of responsible personal use is permitted. This may include calls or texts to family members, child care services or other important non-work related matters.

Responsibility for non-departmental data on mobile devices lies with the device holder. The department and CenITex have no obligation to support the camera function on mobile devices, or to recover or copy non-business related photographs or data.

Holders of DEDJTR mobile devices can accrue up to \$15 of non-work related charges in any given month without providing reimbursement to the department. If personal use in one month exceeds \$15, it is the responsibility of the device holder to reimburse DEDJTR for any non-work related charges above this limit.

A new system, Tangoe, will be introduced which will help DEDJTR people in easily breaking down their bill to determine which numbers are being used for

personal use. Reimbursing the department will begin three months after implementing this policy in order for the system to be set up, and to allow DEDJTR people to become familiar with the system and people to change their usage habits if necessary.

## 6.1 Internet, applications and social media

As with all dealings during the course of employment, public servants must demonstrate public sector values when using DEDJTR mobile devices.

Any personal data such as applications, photos etc. should not breach any standards listed in the [VPS Code of Conduct](#), DEDJTR policies, telecommunications law and regulations, copyright or other relevant laws. Any non-departmental applications etc. are the responsibility of the device holder and not supported by DEDJTR.

Using the internet, social media or downloading applications for occasional non-work use is permitted however this use should be minimal and must be in accordance with DEDJTR social media policies.


The downloading of games, video and audio files for personal use is permitted, provided there is no direct cost to the department or impact on the performance of the device. Large files such as these can be data intensive to download, and pose a security threat if downloaded from unreliable sources.

## 6.2 Privacy

DEDJTR has access to information contained in accounts pertaining to usage of DEDJTR issued mobile devices. Such information includes the telephone numbers which are called or received, number of MMS or text messages sent and received and volume of data uploaded and downloaded.

This information may be used for the purposes of determining whether mobile phone use is in accordance with:

- this policy;
- any other DEDJTR policies;
- any applicable legislation and;
- the VPS Code of Conduct.

DEDJTR people are required to protect and handle personal information in accordance with the [Privacy and Data Protection Act \(2014\) \(Vic\)](#) .

## 6.3 Travel/roaming costs

By default, international access for voice calls and text messaging is disabled on all DEDJTR mobile devices.

If a DEDJTR person is travelling overseas **for business purposes**, approval for international access may be granted for the period of travel. Contact the Technology Services division to activate the service.

To limit excessive costs when travelling, DEDJTR people who intend to use their mobile device overseas should purchase an international voice plan and data pack. The Technology Services division can assist with the purchase of these packs.

For **personal overseas travel**, approval must be requested from the device holder's line manager to activate international roaming before the travel is due to begin. DEDJTR must be fully reimbursed for all personal voice and data charges incurred whilst overseas.

In all other cases where approval has not been obtained, data roaming must be deactivated on the DEDJTR supplied device before leaving Australia. Any costs incurred will require reimbursement by the device holder.

## 7. Responsibilities

### 7.1 DEDJTR people

All DEDJTR people issued with a departmental device are required to ensure their use does not contravene this policy, any other related policies or relevant law. All device holders must ensure they are aware of all related DEDJTR policies.

DEDJTR mobile device holders must be contactable via their departmental mobile number during normal working hours and at other times as agreed with their manager.

DEDJTR people who have been supplied with a mobile device must ensure that their business mobile number is published in the staff directory. Subject to Deputy Secretary (or equivalent) approval, some DEDJTR people involved in



activities of a confidential or sensitive nature may be exempt from this requirement.

If a mobile device holder takes leave for an extended period, greater than two months, they must discuss their telephony requirements during that time with their line manager prior to the leave period. If the device holder retains their device during the leave period, the department is to be reimbursed for all voice and data costs incurred during this time.

## 7.2 Line managers

Managers are responsible and accountable for ensuring regular monitoring of usage, billing, and cost recovery for personal use by all device holders within their supervision. Unauthorised or excessive usage by DEDJTR people will be addressed by the business unit director and/or manager.

Managers are responsible for the issue of mobile handsets when staff join their area. When a DEDJTR person leaves their area, the device holder's line manager must ensure that all hardware has been returned to the Technology Services division. This includes informing the Technology Services division of transfers or cancellations.

Managers must assess requests by their direct reports to retain DEDJTR-owned mobile devices while on extended leave of more than two months. If the request is granted, it is the responsibility of the manager to keep a detailed record of the discussion and agreement reached.

Any changes in the number of mobile telephones, including losses or thefts, or the transfer of connected devices between staff and movement of any related services must be undertaken in conjunction with the Technology Services division.

## 7.3 Business managers

Business units are responsible for payment of all costs and charges related to mobile devices that have been allocated to their people.

The business manager (or their nominee) is responsible for implementing this policy within their business.

Business managers must regularly review the number of mobile telephony devices in their area to ensure they are still appropriate to their needs. If a mobile device or SIM is not assigned to an individual, the relevant cost centre

manager is responsible for its use and should have a register noting who is using the spare service at all times.

## 7.4 Technology Services Division

The Technology Services division is responsible for:

- the provision of mobile devices to DEDJTR people;
- enrolling all DEDJTR-owned mobile devices into the department's chosen Mobile Device Management (MDM) tool;
- installing corporate applications, such as traveller, as required by DEDJTR;
- commissioning of corporate applications to the app store;
- support of business related device function;
- maintaining a register of all DEDJTR-owned mobile devices;
- repair of DEDJTR-owned mobile devices under warranty;
- secure disposal of mobile devices;
- liaising with Telstra regarding services such as mobile number transfers or international roaming;
- remotely wiping the device via the department's MDM if required; and
- administering and reviewing this policy.

## 7.5 Director

Directors are responsible for:

- approving allocation of devices;
- implementing this policy;
- ensuring that business units are monitoring usage;
- Where the service request is for a director, the decision to approve rests with the device owner's line manager.
- Where the device or service request is for a Deputy Secretary, the decision to approve allocation or purchase rests with the Lead Deputy Secretary for People and Executive Services and;

- Where the device or service request is for the Lead Deputy Secretary for People and Executive Services, the decision to approve allocation or purchase rests with the Lead Deputy Secretary for Financial Management and Technology Services.

## 8. Security

DEDJTR people are responsible for the safekeeping of any department owned device under their control.

For security purposes, all department owned mobile devices must be equipped with appropriate mobile device management (MDM) software. This software enables remote management including tracking and remote wiping of lost or stolen devices.

All department owned mobile devices must have security access features such as PIN or access codes enabled to prevent unauthorised access to the device. Security settings on mobile devices are managed by the department's MDM software.

As mobile devices do not afford the same level of security as a desktop PC, strict adherence to guidelines regarding managing sensitive information, and the department's [Proper Use of Information Technology and Electronic Systems Policy](#) are required. Departmental data is not to be store directly on the device.

The use of the camera/video feature must comply with the [Privacy and Data Protection Act](#), the DEDJTR [Information Security Policy](#) and the [Code of Conduct for VPS employees](#).

DEDJTR does not limit the use of DEDJTR supplied devices on Wi-Fi networks. However, device holders must take due care to ensure the security of data on their device. Due to security threats, the use of a DEDJTR supplied mobile device as a 'hot spot' should be avoided unless no secure WiFi networks are available. When using a mobile device as a wifi 'hot spot' it is the responsibility of the device holder to secure the network connection using a passcode.

DEDJTR people travelling overseas should contact the Technology Services division for advice and review the travelling overseas with a mobile device guide prior to departing, which contains helpful information about security measures with mobile devices while travelling overseas.

## 9. Loss, theft or damage

It is the responsibility of the mobile device holder to take reasonable steps to safeguard a department owned device. Loss of a department owned device leaves the department exposed to unauthorised disclosure of data.

If a device is lost, stolen or damaged, the device holder must immediately report the incident to the service provider, Telstra, and report the loss to their business unit manager. When this is complete, a Lost or stolen PSD incident report must be completed and submitted to the Technology Services division as soon as possible.

In the case of minor damage, such as a cracked screen or broken buttons, the device holder should attend to repair of the device through an authorised reseller. The device holder can then lodge a personal reimbursement claim for the cost of repair. DEDJTR people should contact the Technology Services division for advice about authorised resellers in their area.

The device holder will be responsible for any charges on the device until it is reported lost or stolen to the service provider. Managers may request that the device holder arrange the replacement of the device, particularly if further devices are lost within a short time frame.

## 10. Monitoring and reporting

All device usage will be monitored and usage history will be provided on a monthly basis to mobile device holders and their managers. Business managers and Executive Directors will receive monthly summary reports outlining usage for their business units. Technology services will be responsible for this reporting.

In cases of excessive usage, DEDJTR people will be required to provide further details to verify their use is in accordance with this policy. DEDJTR must be reimbursed for any unauthorised use.

Excessive or unauthorised usage will be determined after considering:

- the normal monthly cost/usage for that person;
- the average cost/usage of a person in that function, branch or group;
- calls made outside normal working hours;
- specific projects and workload for that period and;


- international personal travel usage where voice calls and data roaming was not authorised.

Mobile telephone accounts, including recovery of personal calls made, will be subject to examination by Finance and Technology Services and/or internal auditors.

For more information on monitoring and reporting of mobile device usage please see the Proper use of information technology and electronic systems policy (in development).




## 11. Occupational health and safety

The use of mobile devices in flammable environments is prohibited.

VicRoads advise that using a mobile device while driving can be distracting. Mobile phone use, including manual and visual distraction while driving, increases your chance of being involved in a crash or near crash. DEDJTR people should visit <https://www.vicroads.vic.gov.au/safety-and-road-rules/driver-safety/mobile-phones-and-driving>  for advice on the hazards in relation to mobile devices and driving.

## 12. Breach of policy

A breach of this Policy may result in withdrawal of an allocated mobile/smart phone or device. Proceedings addressing possible misconduct may be instigated in accordance with the following:

- DEDJTR policies
- [Code of Conduct for the Victorian Public Sector Employees](#) 
- Directors code of conduct
- Executive employment agreement
- Contractor agency agreement
- Misconduct under the *Public Administration Act 2004* and/or the relevant employment conditions
- Telecommunications offences under the [Criminal Code Act 1995](#)  (Commonwealth)
- Crime under the [Crimes Act 1958](#) .

## 13. Definitions

**Business manager** refers to a direct report of a deputy secretary, with responsibility for ensuring their group's compliance with administrative and financial processes.

**DEDJTR people** refers to people connected with the department of Economic Development, Jobs, Transport and Resources including employees, consultants and staff of any group that receives corporate support from DEDJTR.

**Director** refers to a divisional lead or the direct report of a Deputy Secretary, with the appropriate cost centre financial delegation.

**Financial delegation** refers to the authority to commit and/or approve expenditure in accordance with the requirements of the Financial Delegations policy.

**iPad** refers to the department's choice of tablet device.

**Manager** refers to a supervisor, team leader or Executive with responsibility for the day-to-day management of an employee or DEDJTR people as defined above.

**Mobile device** refers to any compact device with read/write storage capabilities that can be connected to a computer, including personal electronic devices with data storage such as mobile phones, smart phones, pagers, tablets and wireless broadband devices.

**Smart phone** refers to a mobile phone built on a mobile operating system with more advanced computing capability and connectivity than a standard mobile phone, including over-the-air synchronisation with email, calendar and contacts.

**Tablet device** refers to a compact portable touch screen computing device used predominantly for network access. Examples are the iPad, Android and Windows-based tablet devices.

**SIM** refers to Subscriber Identity Module – A small electronic card inserted into mobile phones or other wireless devices that provides network connectivity and a unique identity to the device, for example, the persons billing details and phone network permissions.

## 14. Related information

[Information security policy](#)

[Bring Your Own Device \(BYOD\) policy](#)

[Social media policy](#)

[Proper use of information technology policy](#)

[DEDJTR Mobility request form \(DOCX, 100.4 KB\)](#)

[Bring your own device request form \(DOCX, 78.6 KB\)](#)

Mobile device private use reimbursement form

[Lost or stolen PSD incident report \(DOCX, 62.0 KB\)](#)

[Mobile device return checklist \(DOCX, 63.0 KB\)](#)

Telstra change of ownership global enterprise and services and consumer transfer requests

[CenITex smart phone and tablet services terms and conditions](#) 

Reimbursement of personal calls

Peter Hansen maintains this page

Page last updated: 6 June 2017

Copyright © 2017