DHHS Mobile Communications and Portable Storage Device Policy

Pertaining to the use of department-owned and personally-owned portable electronic devices connecting to the department's network or hardware.

Audience: All departmental employees and contractors engaged by the department, and any other persons using technology provided by the department

If you would like to receive this publication in another format, please email

BTIM Directorate@dhhs.vic.gov.au

VICTORIA State Government | Health and Human Services

Contents

Purpose

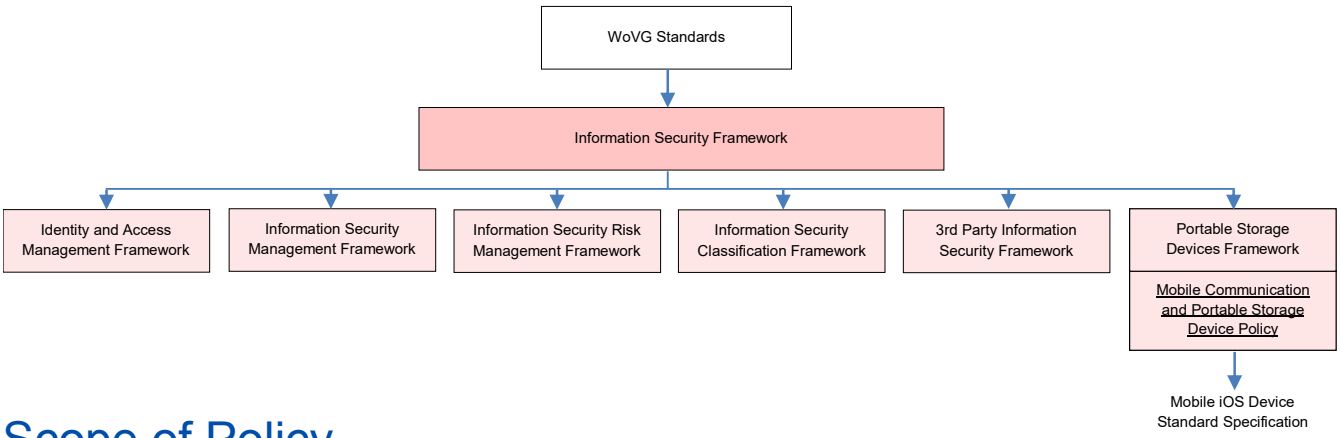
This policy sets out the terms of acceptable use of department-owned and personally-owned portable electronic devices that are connected to the department's network or hardware.

NOTE: Users who wish to use personally-owned technology, including portable electronic devices, to connect to the department's network or hardware must sign terms and conditions setting out the department's requirements, which include adherence to this policy.

Differences in functionality carry significant variation in cost, and this policy and its associated guidelines aim to provide transparency on these functions and costs to allow departmental staff, managers and financial delegates to make the best 'value for money' decision. This policy also governs the requirements that ensure the department's network (including the departmental information stored within it) and hardware remain secure.

This policy is part of the *Portable Storage Devices Framework*, which is a component of the *Information Security Framework* (as shown below) and is to be read within that context.

Figure 1: Information Security Framework



Scope of Policy

This policy applies to the purchase, connection and use of:

(a) mobile communications devices (standard mobile phones); and

(b) portable storage devices, including all devices capable of accessing departmental information. For the purposes of this policy, this includes but is not limited to laptops/notebooks, tablet devices, smart phones /PDAs, USB keys, flash drives, external hard drives, digital audio players, digital cameras and removable media.

Note: 'connection' and 'use' refer to both department-owned and personally-owned devices. This policy does not apply to storage devices used for the formal and scheduled backup of department information.

Interpretation

In this policy, terms have the meaning given to them in the table in Appendix 1.

Policy

1. Policy applicability

All individuals with access to departmental information via a mobile or portable storage device must comply with this policy.

This policy supplements the department's information security management policy and is part of the department's information security framework.

2. General principles

The range of devices covered by this policy will evolve with technology and the security requirements of the Australian and Victorian Governments. As a result, this policy refers to categories of devices, rather than specific types/models (except as examples).

An up-to-date list of approved devices, phone/data plans and accessories can be found in the *Mobile Communications and Portable Storage Device Selection Guidelines, BTIM Service Catalogue* and the *procurement order form*/IBM Form

The following principles apply to all devices, regardless of category:

- **justifiable business need** – the business unit must be able to demonstrate the need for any expenditure related to the purchase and connection of any device
- **multiple devices** – supplying and connecting more than one device for a single user will occur only where there is a justifiable business need for the additional device(s)
- **device-type/model** – only devices deemed appropriate and approved by the Chief Information Officer (CIO) will be supplied or allowed to connect to the department's network or hardware
- **approval** – purchase of the device or connection (including any accessories) must be approved by the appropriate financial delegate
- **provisioning** – devices, connections and any relevant accessories are provisioned by the Information Management and Technology (BTIM) branch
- **occupational health and safety** – the selection and use of any device must be in line with guidelines and recommendations, including consideration of any ergonomic factors (refer to the 'Health, Safety & Support' page on the intranet)
- **personally-owned devices (smartphones and tablets)** –the CIO (or delegate) must approve the connection of any non-departmental device to the department's network or hardware
- **information transfer only** – devices must not be used for the permanent storage of departmental information, but may be used to transfer information or temporarily store copies of information already stored securely in a network location

All devices must meet the hardware, software and security requirements appropriate to the type of departmental information and access they will be used with, as summarised in Appendix 4: 'Requirements for devices approved for use within the department'.

In addition, compliance with category-specific conditions is required. These conditions are listed in the sections that follow.

2.1 Approval levels

The level of approval required for each device type is listed in the Appendix 3. It is important that reasons for approval are recorded and are stored appropriately according to the department's records management policy.

Before an approved device is issued to a user:

(a) the device must be configured for encryption as described in Appendix 4, if applicable; and

(b) the user must have signed the department's terms and conditions setting out the department's requirements for using a departmental device.

3. Mobile communication devices

The table below refers to standard mobile phones, smartphones and personal digital assistants (PDAs), as well as relevant accessories and services.

Table 1: Mobile communication devices and services

3.1	**Standard mobile phones**	In addition to a standard or enhanced desktop phone, a user may be provided with a mobile phone (including connection) where it can be demonstrated that any of the following apply: (a) they need to be frequently contacted and often required to perform duties away from their usual work base (b) they are deployed 'in the field' and require direct contact with their work-unit/client-base (c) there are personal security concerns (for example, staff working alone and away from their usual work base) (d) the requirements of the department are best served by providing the proposed user with a mobile telephone for official use (e) staff are rostered 'on call' and are supporting a critical departmental function Refer to the intranet or the *Mobile Communications and Portable Storage Device Selection Guidelines* for further information.
3.1.1.	**Personal standard mobile phones**	Costs incurred on personally-owned mobile phones related to business use *may* be reimbursed provided they can be justified as incurred in the execution of department-related business. Refer to the *Personal Expenses Policy* for details.
3.2.	**Departmental Smartphones and PDAs**	A corporate smartphone/PDA may be supplied to a user when the need can be demonstrated and the user does not require access to HIGHLY PROTECTED information (as described in the DOH & DHS Information Security Classification – Policy and Standards) as part of their departmental role. Smartphones/PDAs require a mobile data plan to provide a 'roaming connection' that provides connectivity to the department's network. (A smartphone/PDA can utilise a Wi-Fi connection to provide the same connectivity) Refer to the *Mobile Communications and Portable Storage Device Selection Guidelines* for further information. Staff members requesting a Departmental smartphone must sign *Terms and*

		Conditions for Departmental Devices
3.2.1	**Personal smartphones and PDAs**	The department will provide the relevant connectivity services to a personally-owned smartphone/PDA if **all** of the following circumstances are met: (a) there is a valid business need for using the device; (b) the proposed user does not have a departmentally-owned smartphone/PDA; (c) the smartphone/PDA meets the department's compatibility requirements, as detailed in the *Mobile Communications and Portable Storage Device Selection Guideline* document; (d) the staff member signs the *Terms and Conditions for Connecting Personally Owned Devices*; (e) the proposed user member submits a *Set up a Personally Owned Device* IBMForm; and (f) the device is compatible to the security rating of the departmental information to be accessed via the device **Note:** The department will provide technical support for the connection and the department software only. Support and maintenance for the device itself is the responsibility of the user.
3.3.	**Phone features**	Phones will be supplied by the department with the standard features and a number of optional features. Some of the standard features include: • message bank • call waiting • calling number display • wireless communications, that is, Infrared or Bluetooth • SMS (Short Messaging Service) ability – users are reminded that there are costs and character limits associated with SMS. Other services including the following are available at an additional cost: • data capabilities, i.e. GPRS, 1xRTT • other access protocols, i.e. WAP, MMS • international roaming (See: Guidelines for using your mobile overseas) • 'Push to Talk' (subject to handset compatibility).
3.3.1.	**Phone restrictions**	By default, all mobile telephones are barred from calling/accessing the following carrier services: 3. • international • 1900 information • 1902 information

		• 0500 'Follow Me' • 123 (Optus) and 12456 (Telstra) direct connect • Foxtel (Next G service) These restrictions can be lifted on a permanent or temporary basis. A business case, approved by the relevant approver, is required to lift restrictions and must be forwarded to the CIO.
3.4.	**Car Kits**	A 'Car Kit' is only provided to users that travel on department-related business on a frequent basis. Directors can approve the use of a Car Kit in a privately-owned vehicle. This approval must be in writing and include the reasons for the approval.
3.5.	**Phone and data plan payments**	Users supplied with a departmental device, including a phone or data plan, will receive a monthly statement of call and data costs. The user is not responsible for directly paying the monthly statement. The monthly statement must be reviewed for costs associated with personal use. The department will allow private calls on the condition that the department is reimbursed for the cost of all private calls. Payments for private calls must be forwarded to the Financial and Administrative Services Branch, or through the staff member's local Divisional or Regional Finance Unit. The Manager, Corporate Telecommunications, is responsible for making a single payment for all department call-costs to Telstra via the Mobile Phone Payment System (MPPS). Mobile phones that appear on Telstra's bill but are not identifiable by personal, group or business unit name, or have not been registered in MPPS, will be suspended from service without notice, and the department will not be prevented from seeking reimbursement for the bill from the user. A list of current authorised representatives for the MPPS can be found on the intranet.

The *Mobile Communications and Portable Storage Device Selection Guidelines* contains information to assist in selecting the most appropriate device.

4. Laptops, Tablets and Ultrabook Devices

The table below refers to laptops, tablets and ultrabook devices, as well as relevant accessories and services.

Table 2: Laptop, tablet and ultrabook devices

4.1.	**Laptops/Ultrabooks**	A laptop/ultrabook may be provided to a user if the following circumstances are met: (a) a business need for the device can be demonstrated; (b) the laptop/ultrabook is on the list of authorised models and is procured in accordance with the State Purchase Contract via BTIM (refer to the *Mobile Communications and Portable Storage Device Selection Guidelines*) ; (c) the user acknowledges that the provision of the laptop/ultrabook is subject to all applicable department policy, including, but not limited to, the *Acceptable Use of Department's Technology Policy* and the *Mobile Communications and Portable Storage Device Policy*; and (d) the laptop/ultrabook is used in place of a desktop PC. A docking station,

		screen, keyboard and mouse can be provided as part of the provisioning process Once approved, the device is provisioned and supported just like a Personal Computer by the BTIM branch. Staff members requesting a Departmental laptop/ultrabook must sign *Terms and Conditions for Departmental Devices* Note: Personally-owned laptops are not currently supported.
4.1.1.	**Laptop Pool**	The department provides a pool of laptops that are prebuilt and supported by BTIM for business use, including presentations and, project work. The laptops can be connected to the department's network. Contact the IT Service Centre to book the use of these.
4.1.2.	**Wireless Modems**	These devices require a data plan to provide connectivity. The department will provide USB Mobile Network Modems for use with a laptop to enable remote access to email, the internet and the department's network information, providing the following conditions are met: (a) a business need for connectivity can be demonstrated; (b) the user does not have network connectivity to any other departmental-device or a personally-owned device or (c) a business need for multiple connections can be demonstrated; (d) the data plan is approved; (e) the modem is ordered via the *procurement form*; and (f) the device is compatible to the security rating of the information to be accessed via the device. Data plans currently available are listed on the BTIM Service Catalogue.
4.2.	**Departmental Tablet Devices**	Users may be provided with a tablet device where: (a) a business need for having any of the following can be demonstrated: (i) constant access to their email and calendar, (ii) the requirement to access documents remotely, with only minor requirements for editing. Or (iii) producing documents remotely; (b) the user does not already have a departmentally-owned laptop with remote access or any other device with network connectivity or (c) a business need for multiple connections can be demonstrated; (d) the device is on the list of authorised models and is procured in accordance with the State Purchase Contract refer to the *Mobile Communications and Portable Storage Device Selection Guidelines*; and (e) the staff member acknowledges that the device is subject to all applicable

		department policy, including this policy and the *Acceptable Use of the Department's Technology Policy*. Once approved, the device is provisioned by the BTIM branch. More information about the selection of a tablet can be found in the *Mobile Communications and Portable Storage Device Selection Guide*. Staff members requesting a Departmental tablet must sign *Terms and Conditions for Departmental Devices*
4.2.1.	**Personal Tablet Devices**	The department will allow connection of a personally-owned tablet device if **all** of the following circumstances are met: (a) a business need for connectivity can be demonstrated; (b) the device meets the department's compatibility requirements (refer to the *Mobile Communications and Portable Storage Device Selection Guidelines*); (c) the staff member signs the *Terms and Conditions for Connecting Personally Owned Devices* to the DHS network to access DHS information; (d) the proposed user submits a *Set up a Personally Owned Device* eForm; and (e) the proposed user does not have access to PROTECTED information (as described in the DOH & DHS Information Security Classification – Policy and Standards) as part of their departmental role Once approved, the connection is provisioned by the BTIM branch. **Note:** The department will provide technical support for the connection and the department software only. Support and maintenance for the device itself is the responsibility of the user.

5. Other portable storage devices

This refers to devices **OTHER** than those described in sections 3 and 4. Other portable storage devices (PSDs) can be either:

- Items that connect directly to departmental networks or hardware, and can access information , including USB keys, flash drives and external hard drives; and
- Removable media that is inserted into departmental hardware to access information, including CDs and DVDs.

Table 3: Other portable storage devices

5.1.	**Provision of a PSD**	Users may be provided with a PSD where it can be demonstrated that: (a) the proposed user has a business need or requirement to access documents external to the department's network for the purposes of information or demonstration; (b) they do not have any method of connecting to the department's network; (c) the device is on a list of models authorised by the department (refer to the *Mobile Communication and Portable Storage Device Selection Guidelines*); (d) the user acknowledges that the device is subject to all applicable department

		policy, including but not limited to this policy and the *Acceptable Use of Department Technology Policy*; (e) HIGHLY PROTECTED information (as described in the DOH & DHS Information Security Classification – Policy and Standards) is not stored on the device; (f) only copies of information (not originals) are stored on the device; and (g) the device is handled (including its storage and transportation) in accordance with the information security classification level of the information stored on it (as described in the DOH & DHS Information Security Classification – Policy and Standards)
5.1.1.	**Personal PSDs**	The use of personally-owned PSDs (i.e. not provisioned by the department) to store departmental information or to connect to the department's network is not permitted.
5.2.	**Digital Audio Players**	Digital audio players are not permitted to be connected to any department computer or network at any time. The only exception is a personally-owned iPod Touch, which can be used (subject to approval) as an approved, cost-effective alternative to a smartphone/PDA.

6. Device, Network and Information Security

Before any device is issued, connected to the network, accesses departmental information or approved for use, it must conform to all security conditions as stated in the following sections below.

6.1 Responsibilities for information stored on portable storage devices

Department line managers must ensure that:

(a) this policy is implemented within their areas of responsibility;

(b) breaches of the policy are reported and investigated, as required; and

(c) corrective or disciplinary actions are taken to address any breaches, as required.

The general obligations of all parties responsible for the protection of departmental information are described in the *Information Security Classification Policy* and supporting guidelines and the relevant Terms and Conditions applying to the use of department-owned and personally-owned devices. In particular:

(a) Only approved devices can access departmental information (refer to the department's Intranet for the list of approved devices).

(b) A user must not access departmental information on PSDs which the user does not have a 'need to know'. Even if there is a valid 'need to know', departmental information should not be stored on a PSD unless there is a departmental business justification for doing so.

(c) Departmental information stored on PSDs must be appropriately secured:

  (i) departmental information that has been security classified as X-IN-CONFIDENCE and above must be encrypted using a department-approved cryptographic algorithm, and protected using a strong password (see the *Password Policy* for password requirements).

  (ii) departmental information that has been security classified as PROTECTED (or RESTRICTED) must only be stored on a PSD if the device itself is protected using a product which has been evaluated using Common Criteria to at least EAL2. (There are some exceptions to this – refer to Appendix 4)

(iii) **PSDs must not be used for storing information classified as HIGHLY PROTECTED and above.**

(d) When moving, transferring or copying departmental information from one PSD to another, the information in the new location must also be protected in accordance with the *Information Security Classification Guidelines*.

(e) PSDs should be used only to create and transport departmental records in the short-term and these records must be transferred to corporate record keeping systems as soon as practical, and then removed from the devices. All electronic information that is updated and relates to departmental records must be stored securely on the department's network on a relevant database or system in accordance with the DHHS Records Management Policy.

(f) PSDs must not be used for informal backup of departmental systems or departmental information. Formal backup arrangements, approved by department management, must be in place for this purpose.

(g) Departmental information must not be stored on unauthorised internet-based storage technology (including Cloud technologies, Dropbox, Box, Google Drive, and Apple iCloud).

Important:

Departmental information must never be moved or copied from a PSD when working on that departmental information at home or when travelling. Accessing information in a document or file must be done on the approved device itself, and not on the hard drive of an unapproved computer. This ensures any temporary copies of the file created by any software remain on the approved PSD.

In situations where temporary files are authorised to be created on an unapproved device, those files must be deleted when the work is complete and the Recycle Bin or Trash folder immediately emptied.

The department reserves the right to ensure that all personally-owned devices no longer contain departmental information in the event of a security incident, role change that does not require access to departmental information, prior to departure of employment, and in any other scenario considered appropriate by the department.

The user should not have any expectation of privacy in relation to their use of a departmental device. The User must not delete any logs or records on or within departmental devices that are associated with actions undertaken while using the device, including call histories, SMS' and iMessages. Logs and records on or within devices may be used by the department in investigations, court proceedings and disciplinary matters which may or may not involve the relevant user.

7. Physical Control and Security of Portable Storage Devices

Only PSDs approved for use within the department should be provided to department staff issued by BTIM / IT Service Centre. All department-owned PSDs must be registered as being in the custody of the relevant user.

Other than when a PSD is used to transfer, with approval, departmental information to another party (for example, a presentation on a CD):

(a) the device must remain in the custody of the user the device was issued to, and recovered by the department from the same user.

(b) users must not allow their PSD to be used by another individual, including fellow staff.

The responsibility of protecting the device (including a personally-owned device), and any departmental information accessed via it, lies with the user who is approved to use the device in accordance with this policy.

7.1 Labelling

All departmental-owned PSDs must be clearly labelled *IN-CONFIDENCE. Property of Department of Human Services. If found, contact <telephone number>".* This will be done by the Workspace Support team. The use of any device not carrying this statement is prohibited unless otherwise approved in writing by the relevant Executive Director.

7.2 Loss or theft

PSDs are considered attractive items and are therefore targets for theft. If a PSD is suspected to be Lost or stolen, the user must immediately report the suspected loss or theft to their line manager and the IT Service Centre, who will act in response to the report. If remote wipe facilities are available for the device, they must be activated. All user accounts associated with a Lost or stolen device must also be reset.

7.3 Storing PSDs

When not in use and not in the personal custody of the user, the PSD should be stored in accordance with the *Information Security Classification Guidelines*:

(a) PSD backups must be stored separately from the device itself

(b) The PSD user should make every effort to secure the PSD when not in their personal custody. PSDs with sensitive or classified information must be stored in accordance with the requirements commensurate with the security classification level of the information accessed via the device (including storing the device out of common sight and locking the device in a secure container left in a secure location within the department's premises), especially devices that access PROTECTED level information.

(c) the keys or access codes to any locked containers used to store a PSD must be effectively secured as follows:

  (i) keys must either be in the personal custody of the user, or stored in a key cabinet in the custody of a departmental staff member that has been approved by the department to store the keys. Keys must not be left hanging in or near the container, or in a place that is otherwise easily accessible to unauthorised users; and

  (ii) codes must be known only by the device user or custodian, and not easily guessed (see the *Password Policy* for tips on strengthening password). Codes should not be written down, unless there is a genuine need to do so in which case they should be sealed in an envelope and securely stored in the custody of a departmental staff member that has been approved by the department to store the envelope.

7.4 Travelling with a PSD

When travelling, the user must ensure additional security measures are implemented to protect the PSD and the information it can be used to access, including:

(a) by ensuring that the device contains only those files that the user needs during their travel activity;

(b) by ensuring that the device is never stored in checked-in luggage (including with airlines and hotel porters), and that the device remains in the physical possession of the user

(c) by ensuring that the device is never stored in a motor vehicle *at any time*.

7.5 Transferring a PSD to another person

Note: Departmental iOS devices can only to be transferred to another person by completing the transfer form. This ensures that the devices is correctly wiped and re-provisioned . When a PSD is transferred to another user:

(a) the other party must be briefed on the relevant requirements for protecting the device and information stored on it, including by giving them a copy of this policy;

(b) the password for encrypted information on the device must be communicated separately and must not be written or stored on the device. It must be a unique password that is used solely for the transfer of information from that specific device; and

(c) the device must be transferred physically in person including via an approved courier or internal mail.

7.6 Role change or termination of user's relationship with the department

When there is a role change or termination of the user's relationship with the department and the department considers that the user no longer requires a device that the user has been using, the department's relevant processes must be promptly and accurately implemented and must include:

(a) the recovery of PSDs from the user, and in the case of departmental devices, a transfer form must be completed;

(b) the wiping of departmental devices;

(c) physical destruction of recovered PSDs or faulty PSDs by BTIM following approved destruction processes; and

(d) the updating of PSD registers to record these activities, as appropriate.

When a PSD is recovered due to a role change or termination, the conditions of the *Information Security Classification Policy* must be followed and:

(i) reusable devices must be sanitised; and

(ii) non-reusable devices must be destroyed.;

For personally-owned devices that no longer require access to departmental information or resources, the user must permit BTIM to clear the device of any departmental information and connectivity and departmental resources, including the removal of mobility access has also been removed. For personally-owned iOS devices, the following de-provisioning process must be implemented:

(i) Desktop Support will perform an Enterprise wipe of their device;

(ii) the user must delete departmental information in collaboration with Desktop Support;

(iii) the user must sync the device via iTunes at home; and

(iv) the user must email confirmation of the home sync verifying that there is no departmental information or material on the devices.

Irrespective of whether or not the above de-provisioning process is implemented, the department may exercise its absolute discretion to wipe the device, including where this may result in the loss or destruction of personal information and intellectual property.

7.7 Accessing information on PSD

Staff must assess the risks of accessing departmental information via PSDs outside of the department's premises. Care must be exercised when accessing departmental information on a PSD in an uncontrolled environment, including public areas.

8. Communications Security

Approved PSD connection methods are summarised in Appendix 4. Unauthorised connection and synchronisation are prohibited.

If connection or synchronisation of a device is approved by the department, device or network authentication must be used to differentiate between known, trusted devices and personally-owned or otherwise un-trusted devices.

If a device is authorised to connect to the department's network using wireless communication, the wireless network must be implemented utilising department-approved Wireless documentation. Please refer to the *Wireless Network Policy, Technical Standard and Guidelines* document for more information.

9. Administration and Support

9.1 Administration

All PSDs approved for accessing departmental information or resources will be registered by BTIM for both administration and support purposes, including the name and contact details of the device user. All transfers from one user to another will also be recorded.

Department administration, maintenance and support staff will be trained in the administration and risk management of PSDs.

Authorised IT staff will have remote and direct access to all departmental devices. IT staff access will be audited by the department.

9.2 Repair

If a PSD containing departmental information must be sent for repair to an external party not on the department's premises, the device must be backed up and departmental information removed and sanitised before being handed over to the external party.

9.3 Security patches and software updates

Security patches and software updates must be applied as approved by the department. All laptops, tablets, smartphones and PDAs must be connected to the department's network at least monthly to ensure they have the most up-to-date software and protection.

As these can be large files, the department does not recommend that they are downloaded via the cellular mobile network.

10. Audit and Reporting

The department reserves the right to inspect or audit upon request and at any time:

(a) any departmental device and the information accessed on or via the device.

(b) personally-owned devices that have been approved for use in accordance with this policy, and the departmental information accessed on or via the device.

The department's audit and security officers are responsible for regular audits of PSDs and related software. In particular:

(c) department desktops, laptops/ tablets, smart phones and mobile phones will be regularly audited for unauthorised software;

(d) PSD disposal (including sanitisation and destruction) processes will be regularly audited and, where necessary, corrective actions will be enforced;

(e) a sample of PSD configurations will be audited after changes are implemented to PSDs to ensure the changes have been effective; and

(f) the register of PSDs and their users will be periodically audited for accuracy. This includes auditing the register against the register of lost and stolen PSDs. Any discrepancies must be reported to the relevant information owner (or delegate) and the IT Service Centre. Disciplinary action may be initiated against any department staff who fail to report such security incidents.

Auditors and security officers must notify the relevant information owner or delegate of all security incidents, breaches, or non-compliance with this policy, within one week of completing the audit. Breaches must be reported immediately.

11. Remote Access

Remote access may be provided for devices that are used in locations where a direct connection to the department's network is not possible (including hotels and when users are working from home). Refer to the 'Remote computing service guide' page on the intranet for further details.

12. Access to VicMin

VicMin is the email and calendar service for Ministers and Ministerial staff. The Chief of Staff in the Premier's Office must review and approve/deny all requests for tablet and smart phone devices requiring access to VicMin.

13. Acceptable Use

Departmental-issued mobile communications / portable storage devices and personally-owned devices that access departmental information or the department's network and resources are considered 'departmental technology' under, and their use is subject to, the *Acceptable Use of the Department's Technology Policy* and this policy.

Reasonable personal (that is, non-work-related) use of departmental devices and connections are permitted but should be limited to occasional use and are subject to the *Acceptable Use of the Department's Technology Policy.*

14. Asset Registration and Disposal

All departmental-owned mobile communication or portable storage devices and associated turbo cards and accessories must be registered as assets and disposed of in accordance with the department's *Information Security Classification Policy* and all associated procedures. Refer also to the *Portable and Attractive Items Policy* and the *Disposal of Assets Policy*.

These devices should only be replaced in any of the following circumstances:

(a) the device is at least three years old;

(b) it is considered uneconomical to repair the device; and

(c) technology advancements/improvements warrant replacement of the device and the replacement is approved by the appropriate financial delegate.

15. Monitoring and Enforcement

Policy compliance monitoring and enforcement is the shared responsibility of the department management and BTIM. There will be routine monitoring of departmental devices and personally-owned devices to ensure compliance with this policy.

Reported breaches of this policy will be dealt with in accordance with the department's performance policies and processes.

Policy violation by third parties will be dealt with in accordance with the terms and conditions of the parties' relationship with the department.

Appendix 1: Definitions

The following definitions apply to terms used in this document:

Term	Description
Access	Includes creating, viewing, collecting, downloading, modifying, storing, transferring, processing and sending the whole or any part of information or software, as the context requires.
Backups	A **backup**, or the process of **backing up**, refers to the copying and archiving of data so it may be used to restore the original after a data loss event.
Car Kit	An accessory that allows a user to use a mobile phone hands-free in the car. The kit usually includes a battery charger and a hands-free holder. It may include connections to an external antenna, external speaker or a data port for fax and modem connections.
Common Criteria	Internationally recognised criteria for security evaluations of information and communication technology products. Evaluations are performed in accordance with the international standard ISO 15408.
Department	Refers to the Department of Human Services, inclusive of all Divisions, Branches, Units and Teams.
Defence Signals Directorate	An intelligence agency in the Department of Defence who advises the Victorian Government on matters relating to the security and integrity of information.
Departmental device	A device, including technology, which is provided by the department to a user on a temporary basis for the conduct of the business of the department as a government body.
Departmental information	Any and all departmental intellectual property, information or data which: • has been or is created, acquired, collected, developed, modified, or stored at any time by, on behalf of, or for, the department; • may be in an electronic form or recorded in a tangible form; • may be confidential; • may be protected by intellectual property rights; and • may be accessed by using the device.
Device	A departmental device, or a personally-owned device, or both, as the context requires.
Digital audio player	A small, portable device dedicated to playing computer files containing audio data (e.g. MP3, MP4 and WMA files).
EAL	Evaluated Assurance Level, being an assurance level on the Common Criteria assurance scale.
Information Owner	The department's Secretary who is ultimately responsible and accountable for the security of all information collected, stored and used by the department. Refer to the *Information Security Management Framework* for information about this group and further details on the governance structure.
Laptop or notebook	A device with a fold-up LCD display and keyboard with internal computing capacity.

Term	Description
Mobile Phone Payment System (MPPS)	The payment process for the department's mobile phone account through Oracle Financials.
MPPS	See 'Mobile Phone Payment System'
Encryption	Encryption is the process of systemically encoding data before transmission and during storage so that an unauthorised party cannot decipher it. Distinction should be made between hardware-based and software-based encryption. Hardware-based encryption is forced on the user; whereas software-based encryption gives the user the choice of whether to do so or not.
Lost	When a user is unable to ascertain the location of their device within a maximum 24-hour period
malware	Malicious software including viruses, worms, trojans, backdoors, etc.
PDA	Personal Digital Assistant. See definition for 'Smartphone'.
Personally-owned device	A device that is not owned by the department but that the department permits to be used by a user in accordance with this policy and the terms and conditions that the user has accepted in relation to the use of the device.
Portable storage device (PSD)	Any portable device which contains department information, including USB drives, floppy disks, CDs/DVDs, digital audio players, mobile phones, smart phones, PDAs and laptop computers as well as removable media.
PSD	See Portable Storage Device.
ReadyBoost	A component of the Windows Vista and Windows 7 operating systems that allows for caching of all data on the computer's hard disk to a USB key/drive or memory card.
Removable media	Storage media that can be easily removed, e.g. portable hard drives or digital portable media such as CDs and DVDs.
Tablet device	A device with a touch screen display with internal computing capacity.
Smart phone	A device with the capacities of a standard mobile phone with advanced capabilities including access to data services (eg. Apple iPhone, Android, Windows Mobile).
Standard mobile phone	A device which provides the ability to send and receive mobile phone calls and SMS.
Technology	Workstations, computers (including laptop computers), email accounts and access, network services and connections, internet connections, personal digital assistants (PDAs), portable memory or storage devices, mobile smart devices, tablets, multi function devices (MFD), contracted or approved third party services, and any related IT systems.
Ultrabook	A thin and lightweight device with internal computing capacity
USB drive/key	Universal Serial Bus. Also known as 'flash drive', 'USB stick', or 'memory key'. A storage device that plugs into the computer's USB port. Small and readily concealed, it allows data to be easily downloaded to the device.
User	Any individual who uses the technology resources or services provided by the department.

Appendix 2: Related Documents and Policies

A. *Acceptable Use of the Department's Technology Policy* – This policy outlines responsibilities when using the technology resources and services provided by the department.

B. Australian Government Office of the Australian Information Commissioner (2009), *Public Sector Information Sheet 3 – Portable storage devices and personal information handling* – This document provides suggestions for safeguarding personal information stored or handled on portable storage devices.

C. *Clear Desk and Clear Screen Guidelines* – This document provides guidelines for protecting the workspace to prevent unauthorised access to the departmental information.

D. Code of Conduct for Victorian Public Sector Employees (No.1) 2007 – The Code of Conduct applies to all public sector employees pursuant to the *Public Administration Act 2004* (Vic). The purpose of the Code of Conduct is to promote adherence to public sector values by public sector employees.

E. *Conditions of Use for RSA Enabled Computers* – This document provides advice on the conditions of use applicable to department staff using Remote Secure Access (RSA) to the department's computer network from any location not under the control of the department.

F. *Disposal of Assets Policy* – This policy outlines the requirements and transactions in relation to the treatment of an asset and depreciation when the asset is disposed of prior to attaining its depreciable life.

G. *HSNet Access Control Policy* – This policy outlines the conditions and standards that apply to connecting to the department's network through any means and for any purpose.

H. *Information Security Classification Policy* – This document provides policy and standards requirements for the management and protection of security classified information, including clear desk and clear screen practices.

I. *Information Security Framework* – This document provides the context for all information security related policies and supporting documents.

J. *Information Security Management Policy* – This policy sets out security requirements for information created, processed, held, maintained or transmitted by the department.

K. *Mobile Communications and Portable Storage Device Selection Guidelines* – Guidelines for selecting the most appropriate device for use with the *Mobile Communication and Portable Storage Device Policy.*

L. *Password Policy* – This policy sets out the requirements for creating and using passwords across all devices that access department applications and information.

M. *Personal Expenses Policy* – The purpose of this policy is to ensure that employees incurring personal expenses are aware of the correct procedure for completing claims.

N. *Portable Storage Devices Framework* – includes information about the use of mobile communication and portable storage devices with departmental information or access to the department's network.

O. *Portable and Attractive Items Policy* – This policy covers the policy and process of accounting for Portable and Attractive Items. This policy does not cover Oracle financials or Oracle Fixed Asset module processes and procedures.

P. *Privacy Policy* – This sets out the Department's policy in relation to protecting the privacy of personal information, in conjunction with applicable privacy laws.

Q. *Staff responsibilities when using the remote computing service (PDF 233.1 KB)* – This document provides additional information for remote access to the department's network.

R. *Telecommunications Policy* – This policy provides an overview of the management of telecommunication services within the department.

S. *Terms and Conditions for Connecting Personally Owned Devices* – This form must be completed prior to a personally-owned device being connected to the department network.

T. *Terms and Conditions for Departmental Devices* – This form must be completed prior to a corporate device being provisioned to a DHS staff member.

Appendix 3: Required Levels of Approval

The following table lists the approvers for the various devices:

Device Type	Approval Level
Standard mobile phone	Appropriate financial delegate
Smartphone/PDA	Director
Connecting personally-owned devices e.g. Smart Phones, PDAs, or Tablets	Director
Access to non-standard phone features	Director
Lifting restrictions to carrier services	Director
Car kits	*Government* vehicles: Financial Delegate *Private* vehicles: Director
Laptops,Tablets and Ultrabooks	Director
Wireless modem	Director
Data plan	Director
Other portable storage device or removable media	Financial Delegate
Connecting personally-owned portable storage device or removable media	Not permitted
International Roaming (Voice Plan and Data Plan)	Director

Refer to the *Mobile Communications and Portable Storage Device Selection Guidelines* for information to assist with selecting the most appropriate device.

Appendix 4: Requirements for PSDs approved for use within the department

Device Type	Requirements	Approved Classification	Approved Connection
Standard Mobile Phone (non-Smart phone)	• Software controls must enforce 'PIN' (password) feature of the device	Up to UNCLASSIFIED Only used for voice and SMS.	N/A
Corporate Apple iOS Device (iPhone, iPad) Corporate Standard Profile	All iOS Devices must be managed by Mobile Device Management (MDM) software. Refer to the Mobile iOS Technology Standards for more information regarding: • Device Settings including passcode policy and restrictions. Policies are enforced by the MDM and vary based on profile. • Supported device models and operating system versions • Standard Operating Environment (SOE)	Up to X-INCONFIDENCE	Connection of approved devices to department networks using the appropriate security controls, e.g. SSL VPN is permitted (where authorised by the department). Refer to the Mobile iOS Technology Standards for more information.
Corporate Apple iOS Device (iPhone, iPad) Corporate Confidential Profile	All iOS Devices must be managed by Mobile Device Management (MDM) software. Refer to the Mobile iOS Technology Standards for more information. The Corporate Confidential profile is generally more restrictive than the Corporate Standard profile, e.g. stronger passcode policy, users do not have the ability to install apps themselves etc.	Up to PROTECTED	Connection of approved devices to department networks using the appropriate security controls, e.g. SSL VPN is permitted (where authorised by the department). Refer to the Mobile iOS Technology Standards for more information.
BYOD Apple iOS Device (iPhone, iPad, iPod Touch) BYOD Standard Profile	All iOS Devices must be managed by Mobile Device Management (MDM) software. Refer to the Mobile iOS Technology Standards for more information.	Up to X-INCONFIDENCE	Connection of approved devices to department networks using the appropriate security controls, e.g. SSL VPN is permitted (where authorised by the department). Refer to the Mobile iOS Technology Standards for more information.

Device Type	Requirements	Approved Classification	Approved Connection
Corporate Laptop/Ultrabook computers	Hardware Requirements • Laptops that contain data classified 'highly protected', 'confidential' and above must be fitted with a physical device lock. • Unused ports and interfaces must be disabled. Software Requirements • Software that performs 'pre-boot' encryption. The total disk must be encrypted using McAfee Total Protection for Data • A configured personal firewall in addition to anti-virus and malware software suite software that can block/deny/decline unauthorised wireless connections	Up to HIGHLY PROTECTED	Connection of approved devices to department networks via the department remote access services is permitted (where authorised by the department).
Corporate USB Drives	• The total disk must be encrypted with Encryption software	Up to PROTECTED	N/A
Optical Discs (e.g. CDs, DVDs)	• Data stored on discs should be encrypted with the appropriate level of strength commensurate with the data sensitivity of the information.	Up to X-INCONFIDENCE	N/A

Document Control

Contact details:	Directorate, BTIM, Corporate Services 50 Lonsdale Street, Melbourne BTIM Directorate@dhs.vic.gov.au

Version history:

Version	Date	Updated by	Summary of changes
0.6	19Nov09	R Lambert	Baseline document "DOH & DHS Portable Storage Devices – Policy, Standards & Guidelines"
3.0		K Henderson	Information on mobile communication devices split out and new document created – "Mobile Communication Devices Policy"
5.0	26Nov11	K Henderson	Information on Acceptable Use added
5.1	22Aug11	N Chaperon	Title change to "Mobile Communication and Portable Storage Device Policy". Inclusion of all forms of device and reference to network/data security. Appendices moved to accompanying guidelines document.
5.2	25Aug11	N Chaperon	Replaced specific references to DHS and added definition of 'department'. Inclusion of additional related documentation.
5.3	30Aug11	N Chaperon	Minor updates to information on laptops; document control added.
5.4	02May12	N Chaperon	Updated to reflect framework & OHS considerations; incorporated elements of the *Portable Storage Devices Policy*; added info on remote access.
6.0	Jan13	R Tall	Updated relevant sections as part of the "Mobility" project (that is, the deployment of DHS infrastructure to securely control DHS and personally owned iOS devices.
6.1	Feb13	S Crabb	Updated following Legal review and Appendix 4 changes
6.2	March13	S Crabb	Minor Changes
7.1	Aug 14	I King	Minor changes – updated smart phone definition, removed BlackBerry references
7.2	22 Jun 15	D Guarnaccia	Added Ultrabook
7.3	05 Aug 15	D Guarnaccia	Updated Appendix 3 – Required levels of approval
8	23 Sep 15	D Guarnaccia	Feedback incorporated from Business Engagement and Service Delivery – and finalised
9	11 Oct 16	D Guarnaccia	International Roaming approvals

To receive this publication in an accessible format phone 9096 7511, using the National Relay Service 13 36 77 if required, or email BTIM.Directorate@dhhs.vic.gov.au

Authorised and published by the Victorian Government, 1 Treasury Place, Melbourne.