[Information Management and Technology Policy](http://intranet.health.wa.gov.au/ips/imt_policy/index.cfm)

# TITLE: PORTABLE COMPUTER AND STORAGE DEVICES POLICY PURPOSE

The purpose of this policy is to implement a uniform and consistent approach to the allocation, access and usage of portable computers and associated storage devices for business purposes.

This policy is an adjunct to the Your Company Acceptable Use Standard – Information Communications and Technology (ICT), which defines the acceptable behaviour expected of users and intending users of Your Company ICT resources.

# SCOPE

This policy applies to all staff within Your Company and Your Company entities.

This policy covers **portable computers** owned or leased by Your Company including (but not limited to):

* Laptops/notebooks
* Tablet PCs
* Personal digital assistants (also known as PDAs, Pocket PCs)

**AND storage devices** including (but not limited to):

* USB flash drives
* Flash cards
* Cameras
* Media players
* Optical (CD and DVD) disks
* Magnetic disks (floppy and external hard drives).

# POLICY STATEMENT

1. **Purchases or lease of portable computers (not storage devices) must be approved by the CIO.**
2. **All portable computers must be purchased via and comply with procurement policies**
3. **Portable computing and storage devices used for Your Company purposes must have designated custodians who are responsible for the protection of the physical device and any stored or accessed information.**

**GUIDELINES TO ASSIST WITH POLICY COMPLIANCE**

**ALLOCATION**

Your Company entities may only allocate portable computing devices (particularly laptops) to personnel with demonstrated business need. The provision and ongoing use of portable computing devices is to be based on a range of operational criteria including, but not limited to, the following:

* there is a frequent requirement to use the device for mobility purposes; or
* staff are not based at any one particular site and access to alternative devices (e.g., desk top PC) at their work location is not available or cannot be economically provided.

Requests for the specific purchase and allocation of a portable computer device to an individual or work group will require endorsement by the Chief Information Officer on the recommendation of the Divisional Head/Executive Director.

Portable computer devices must be purchased in accordance with our purchasing standards. In general, base models will be purchased unless there is a justified need for a higher level specification model.

# ACCESS TO THE YOUR COMPANY NETWORK

Authorisation to use portable computing devices to access Your Company computing and communication resources and information will only be granted if the hardware and software comply with Your Company’s Managed Operating Environment, and where virus protection and security software patches are installed at the current levels. Only in exceptional circumstances will non-Your Company owned devices be permitted to connect to the Your Company network and only then where these devices also meet Your Company requirements for virus protection, security or operating system software levels.

Users of any portable computing devices (Your Company or permitted third-party), which are not regularly connected to the Your Company network, must consult with the ICT to verify that the devices are virus-free or that current versions of security patches and virus software are installed on these devices before reconnection to the network.

ICT staff must ensure that third parties allowed access to the network have and maintain appropriate security patches, operating systems and virus protection levels on their portable computer devices.

Your Company reserves the right to implement manual or automated controls to detect non- compliant devices and to deny or cancel Your Company network access. Your Company also reserves the right to implement tracking or location management measures such as radio frequency identification (RFID) tags on Your Company owned devices.

# DATA MANAGEMENT

Your Company personnel are accountable for their use of the portable computing devices and are responsible for the secure storage, backup, transmission, access and disposal of information contained on these devices. These responsibilities include compliance with legislative and other policy requirements. Users who breach these requirements may be subject to disciplinary action and other punitive measures available through legislative provision and the Criminal Code where appropriate.

Your Company personnel must be circumspect in the use of portable storage devices. Unsecured devices must not be used to store or transport unencrypted sensitive Your Company data.

Secure methods must be used for the transmission of sensitive data. Security risks associated with wireless communications must be addressed before data is transmitted.

Portable storage devices must be scanned for detection and removal of malicious software before data is transferred from these devices to any Your Company networked device.

Secured Application and Database Servers housed on Your Company ICT facilities are the designated primary Your Company data means of storage. Where portable computer and storage devices are used for the capture or transport of original data, such data must be transferred to primary storage as soon as practicable.

# DEVICE CARE

Measures must be taken to protect portable computer and storage devices from unauthorised use, destruction, or theft.

Staff have an obligation to use their allocated portable computing and storage devices in a responsible, informed and safe manner. Staff are responsible for the security of the devices at all times and may be held liable for any negligence resulting in lost, stolen or damaged units. Devices should not be left at risk in vehicles or in unsecure locations.

In the event of a device being lost or stolen, the following immediate actions are to be undertaken:

* Report the loss to the relevant local ICT and relevant business units
* If stolen, report the loss to the QLD Police Department, and obtain an official report number for insurance purposes.

Any delay in reporting the loss, which results in misuse of the device, may contribute to the officer being held responsible for any costs or damages.

# CENTRAL INVENTORY

A register of all approved portable computing devices will be maintained by ICT and will include the following information:

* Officer's Name
* Location (branch/section)

* Make / model
* Serial number.

# DEFINITIONS

NA

# BACKGROUND

The use of portable computing devices is governed by Your Company policies and procedures for their safe, secure and authorised operation.

Portable computing devices have the capacity to significantly and positively impact the Your Company working environment and service delivery. Their widespread use, however, requires application of appropriate controls to reduce the potential risks they pose to Your Company information and infrastructure by being easily accessed, misplaced, damaged or stolen.

Your Company has a duty and responsibility to ensure that its information is protected from harm, unauthorised or inappropriate disclosure, while at the same time ensuring that it is available to those who have a legitimate right or need to know. Use of portable computing devices also increases the risks of the introduction of viruses and other undesirable intrusions to the Your Company IT infrastructure, the prevention of which requires additional security controls.

While portable computer devices can help staff manage information more efficiently, especially when they are outside their normal office environment (e.g., when travelling interstate or otherwise off-site), it must be noted that the provisioning and support costs for these devices are higher and they have a shorter life span than desktop computers. Therefore, desktop computers must be used where possible.

Portable computer devices with wireless capabilities may interfere with other equipment. Some settings may require these devices to be turned off where there is potential for interference with medical equipment.

Users must ensure safe use of these devices to protect themselves and others from potential harm and also observe laws associated with their use. Different jurisdictions may have differing legislation governing their use and requirements. Users should familiarise themselves with the requirements of these jurisdictions when travelling on Your Company business.

Users of portable computing devices must take care not to blur the boundary between personal and corporate ownership or use. This requires a heightened awareness of the risks involved to protect both the individual and Your Company from the unintended consequences of their use.

# IMPLEMENTATION

Divisional Heads and Executive Directors are responsible for ensuring that staff:

* are aware and periodically reminded of their obligations to ensure appropriate, secure and safe use of portable computer devices; and
* follow proper procedures when purchasing, allocating and using portable computer devices.

All portable computing device allocations are to be reviewed annually in accordance with this policy. All new requests for additional or replacement portable computing devices will be assessed against this policy.

Where current allocations are no longer deemed appropriate, devices should be returned to ICT immediately.

An audit of the central register will be conducted by ICT on an annual basis, with a summary report and recommendations for efficient and accountable ongoing management of portable computing devices to be submitted to the Chief Information Officer.

**REVIEW**

In order to ensure currency and ongoing relevance to Your Company, this policy will be reviewed on a 2 yearly basis.

# VERSION CONTROL

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Purpose:** | Ensure the appropriate purchase, allocation and use of portable computing and storage devices. | | | | | |
| **Relevant To:** | Your Company | | **Approval Authority:** |  | | |
| **Effective Date (Approved):** |  | **ICT**  **Approved Date:** |  | | **Expiry Date:** | To Be Advised |
| **Responsible Group**: | Information Policy | | **Enquiries Contact:** | |  | |
| **Summary of Changes From Original Version** | | | | | | |