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 WA Health Acceptable Use Standard – Information Communications and Technology (ICT), which defines the acceptable behaviour expected of users and intending users of WA Health ICT resources.

SCOPE
This policy applies to all staff within WA Health entities including:
- Department of Health
- Metropolitan Health Service
- WA Country Health Service.

This policy covers portable computers owned or leased by WA Health 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. Application for approval to buy a new or replacement portable computer is via HFN-070 which must be completed and sent to Director, Service Delivery, Health Information Network (HIN) either via fax or e-mail.
3. All portable computers must be purchased via and comply with DTF CUA 16503B.
4. Portable computing and storage devices used for WA Health purposes must have designated custodians who are responsible for the protection of the physical device and any stored or accessed information.

REMEMBER

Staff should consult this policy regularly to ensure that their activities conform to the most recent version, which is held on the Information Management and Technology Policy intranet site, other policies mentioned in Associated Policies, Standards, and Guidelines should also be periodically reviewed for later versions.
GUIDELINES TO ASSIST WITH POLICY COMPLIANCE

ALLOCATION
WA Health 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., desktop PC) at their work location is not available or cannot be economically provided.

Each local ICT group will hold a small pool of laptop computers for short term loan to meet occasional travel and presentation requirements.

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 State Government and/or DOH mandatory contract arrangements. In general, base models will be purchased unless there is a justified need for a higher level specification model.

ACCESS TO THE WA HEALTH NETWORK
Authorisation to use portable computing devices to access WA Health computing and communication resources and information will only be granted if the hardware and software comply with WA Health’s Managed Operating Environment, and where virus protection and security software patches are installed at the current levels. The Health Information Network ICT (ICT) is responsible for oversight and direction of the Managed Operating Environment. Only in exceptional circumstances will non-WA Health owned devices be permitted to connect to the WA Health network and only then where these devices also meet WA Health requirements for virus protection, security or operating system software levels.

Users of any portable computing devices (WA Health or permitted third-party), which are not regularly connected to the WA Health 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.

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

---

1 This may apply for a government or non-government user who has a legitimate requirement to access the health network, and only where it is determined by the IT Group that it is not practical for that person to use a WA Health-owned device.
DATA MANAGEMENT
WA Health personnel are accountable for their use of the public sector’s 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 such as the Public Service Regulations and the Criminal Code where appropriate.

WA Health personnel must be circumspect in the use of portable storage devices. Unsecured devices must not be used to store or transport unencrypted sensitive WA Health 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 WA Health networked device.

Secured Application and Database Servers housed on WA Health ICT facilities are the designated primary WA Health 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 WA 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)

Sensitive data includes identifiable personal and confidential business information.
DEFINITIONS
NA

BACKGROUND
The use of portable computing devices is governed by Department of Health and WA public sector policies and procedures for their safe, secure and authorised operation.

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

WA Health 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 WA Health 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 desk top computers. Therefore, desk top computers must be used where possible.

Portable computer devices with wireless capabilities may interfere with other equipment. Hospital 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 WA Health 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 WA Health 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.
Portable Computer and Storage Devices Policy

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.

REMEMBER

WA Health requires users to accept the ICT policies, standards and guidelines governing the use of the ICT facilities as a condition of their use. These are accessible via the intranet at Information Management & Technology Policy.

REVIEW

In order to ensure currency and ongoing relevance to WA Health, this policy will be reviewed on a 2 yearly basis by the Health Information Network.

ASSOCIATED POLICIES, STANDARDS AND GUIDELINES

Associated IM&T policy can be located on the Information Management and Technology Policy intranet site:

- Acceptable Use Standard – Computing and Communication Facilities
- Information & Communications Technology (ICT) Procurement Policy and Guideline

RELEVANT LEGISLATION

NA

VERSION CONTROL

<table>
<thead>
<tr>
<th>Purpose:</th>
<th>Ensure the appropriate purchase, allocation and use of portable computing and storage devices.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relevant To:</td>
<td>WA Health</td>
</tr>
<tr>
<td>Approval Authority:</td>
<td>SHEF</td>
</tr>
<tr>
<td>Effective Date (DG Approved):</td>
<td>21 May 2009</td>
</tr>
<tr>
<td>SHEF ICT Approved Date:</td>
<td>March 2009</td>
</tr>
<tr>
<td>Expiry Date:</td>
<td>To Be Advised</td>
</tr>
<tr>
<td>Responsible Group:</td>
<td>Information Policy</td>
</tr>
<tr>
<td>Enquiries Contact:</td>
<td>Manager, Information Policy (08) 6213 5406</td>
</tr>
</tbody>
</table>

Summary of Changes From Original Version

July 2009 – Added policy statements and link to Form 070 and CUA 16503B.