## ITKM Hardware Asset Management Policy

### 1   Purpose

The purpose of this policy is to ensure that all ITKM hardware in use throughout the University is correctly managed and can be proven to be so.

The use of ITKM Hardware is fundamental to operation of the University and as such the University maintains a large investment in technology. The fact that much of this technology is often portable, highly dispersed and may hold large amounts of corporate information requires that it be closely managed.

The ITKM Hardware Asset Management Policy addresses the following aspects of the asset lifecycle:

**Planning:** The bulk of ITKM assets to be procured and retired will be identified through the Universities annual planning cycle which in itself will draw upon the University's asset database.

**Acquisition:** The procurement of ITKM assets from capital budgets will be managed by the ITKM Department on an annual basis. The ITKM Department will provide a 'catalogue' approach of approved configurations for commodity items (PCs, laptops etc) which will also be used for ad-hoc revenue purchases. This will ensure all ITKM equipment is procured efficiently, in compliance with financial regulations and with appropriate warranties.

**Deployment:** Data bearing portable computing devices (Laptops, Tablets, smartphones, Ironkey's etc) will always be deployed with encryption enabled by default and always to named individuals.

**Management:** In-service, ITKM assets will be tracked through use of the University's asset database and in accordance with the Asset Manager Procedures. ITKM assets not allocated to named individuals, such as desktop PCs, servers, network equipment etc will be allocated to a location rather than a person. A user driven asset transfer function will simplify the tracking of portable assets between named individuals and sign-post devices to be returned by leavers. Both portable and fixed location devices will be cross-correlated with other information systems to aid location tracking.

**Retirement:** Assets deemed to be of no further use will be written off in line with the Asset Manager Procedures. This will ensure that assets are disposed of with due consideration of data security liabilities and legal disposal requirements.

### 2   The Policy

The University requires that all ITKM hardware, particularly data bearing portable equipment, is properly managed throughout its lifetime.

2.1 This policy applies to all owners and users of University ICT equipment. There are significant legal implications for the individual and the University with respect to breach of this policy.

## 2.2 General Responsibilities of Schools and Departments

**2.2.1** Adherence to the Asset Management Procedures and Financial Regulations noting:

- Proper coding to be used for ITKM asset procurements within the purchase order process.

- ITKM Assets not to be purchased on credit cards, petty cash or from unapproved suppliers without prior consultation with the ITKM Department.

- Data bearing portable computing devices must be purchased from the University ITKM catalogue. Any requirement to deviate from that to be approved by the ITKM Department in advance.

- All qualifying (by value or being data bearing portable computing device) assets to be recorded in the asset database.

- ITKM assets must be marked with an approved asset sticker upon delivery.

- No data bearing portable computing device to be issued without consideration of its secure configuration (encryption) and allocation to a named user.

- Any change of location or custodianship of an ITKM Asset to be recorded in the asset database.

- Recovery and reallocation of ITKM assets from leavers.

**2.2.2** Schools and Departments become custodians of the ITKM assets issued for the use of their staff or students. This custodianship requires that adequate steps are put in place to ensure the security and safety of the assets. This is most easily accomplished by ensuring staff are aware of their responsibilities with regard to looking after ITKM assets. See 2.3.1 below.

**2.2.3** Only the ITKM Department can dispose of an ITKM asset. In so doing the ITKM Department will follow the disposal process as documented in the Asset Manager Procedures.

## 2.3 Responsibilities of the Users of ITKM Equipment

**2.3.1** Staff become custodians of the portable ITKM assets allocated to them for their personal use. In that regard the following should be noted:

- ITKM assets always remain the property of the University. They cannot be given away, thrown away, sold or kept when leaving.

- ITKM assets must never be used by any third party (friends, family, children etc).

- Any transfer of ownership must be recorded in the asset database by the transferee.

- Should any ITKM equipment become lost or stolen it must be immediately reported to the ITKM Department. The ITKM Department may be able to remotely erase certain classes of device to prevent data leakage.

### 2.4 Responsibilities of the ITKM Department

**2.4.1** To retain oversight of ITKM assets in the asset database. This data will be utilized, alongside other information, to aid long term planning for rolling updating of ITKM assets (retirement and replacement).

**2.4.2** To provide guidance on the selection of ITKM equipment based on an understanding of requirements matched against efficient procurement routes. To that end the ITKM Department will establish a catalogue of commodity items which can be procured favourably with due diligence to security requirements, quality and warranty.

**2.4.3** To ensure devices deployed by the ITKM Department are properly asset marked, secured and the fixed location or named user is recorded against the asset in the asset database.

**2.4.4** To ensure that ITKM devices are, where possible:

- Subject to standard build and configuration,
- Kept up to date with security patches and updates,
- Managed within a framework such that the remote application of polices can reflect the information security needs of the University.

**2.4.5** The maintenance of a consolidated record set to aid in locating lost or missing ITKM assets (a correlation of a number of information sources against data held in the asset database).

**2.4.6** To act is the single point of physical disposal for all ITKM Assets. This will ensure the risk of data leakage is minimized, asset records reflect reality and the legal aspects of electrical equipment disposal are managed.

**2.4.7** Individuals in breach of this policy are subject to disciplinary procedures at the instigation of the Dean\Director with responsibility for the person concerned.

## 3 Ownership

**3.1** The Manager, IT and Communications Services (ITKM Department) has direct responsibility for maintaining this policy and providing guidance and advice on its implementation.

# Computer Lab Policy

- ❖ Students must have ID card to use the computer lab.
- ❖ Students must have permission from respective faculty or LAB staff to use the computer lab.
- ❖ Students must have a signed internet agreement on file to access the internet.
- ❖ Users must comply with the terms of the internet agreement. Do not visit inappropriate sites!
- ❖ Do not change default settings.
- ❖ No food or drinks (except water) are allowed in the computer lab.
- ❖ Students belongings (Bags and laptops) are not allowed in lab
- ❖ Software may be installed by Computer Labs staff only. Do not install any software on your own. Files not put on by Computer Labs staff will be routinely removed.
- ❖ Always log off/shutdown the computer when you are finished.
- ❖ Lab users should maintain professional and courteous communication. Electronic devices should be used on a professional level. No obnoxious or belligerent behavior will be tolerated.
- ❖ Students are expected to be on their best behavior in the computer lab. Follow all
  - o school rules and treat everyone and everything with respect!
- ❖ Activities in the lab(s) that are considered by the lab aides to be abusive to the software, hardware, and\or personnel may result in expulsion from the lab(s) and denial of future use of the lab(s).
- ❖ Breaking rules may result in students losing computer lab privileges.
- ❖ Teachers must closely monitor all students and enforce computer lab rules.
- ❖ Teachers are responsible for maintaining an orderly educational environment,
  - o protecting equipment and keeping the computer lab neat.
- ❖ Users should report any issues immediately to laboratory/IT staff.