IT HARDWARE ASSET MANAGEMENT STATEMENT

1.0 INTRODUCTION

The University has made significant investment in its IT hardware assets and an effective asset management process is an important part of the overall control processes necessary to manage IT infrastructure.

Information Technology & Digital Services (ITDS) is the appointed custodian of all University purchased IT assets and the purpose of this statement is to ensure that all University staff understand their responsibility in the effective management of University IT hardware assets, including equipment purchased through research grants.

2.0 SCOPE OF STATEMENT

IT asset management covers all University owned IT assets including all desktop hardware, mobile tablets, devices and software. This statement should be read and understood by all staff their agents and visitors. The use of any UWS IT asset implies an agreement of this statement.

A separate statement covers the control and licensing of software.

3.0 STATEMENT GUIDELINES

ITDS are the authority for the specification, purchase, installation, support and disposal of all UWS IT hardware.

3.1. IT Hardware Purchase

All IT hardware will be purchased in accordance with UWS Procurement protocols and via ITDS to ensure asset registration.

3.2. IT Hardware Maintenance and Support

During the lifespan of the IT hardware asset, maintenance and support will be provided by ITDS, either directly or through a third-party contract.

3.3. IT Hardware Refresh

Where a hardware refresh budget has been allocated, a rolling programme of replacement will take place, prioritising the oldest equipment first. The hardware refresh process may also include a cascade of equipment that is not life expired.

3.4. IT Hardware Disposal

All IT hardware assets, which ITDS consider life expired, should be removed from service and not relocated or brought back into service. All IT disposals will be carried out in a manner compliant with the relevant legislation and institutional policies, in particular the Waste Electronic & Electrical Equipment (WEEE) Regulations 2006 and General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)

3.5. IT Hardware Asset Registration

As part of the issue or installation of new IT hardware, details of the equipment will be recorded in the university's asset register. A unique ID number will be allocated for each asset and details recorded with the 'principal user' of the asset and its location prior to distribution.

3.6. IT Asset Security

It is essential that the physical security of all IT hardware assets be maintained and it is the responsibility of all staff to be mindful of IT hardware assets in their possession, particularly where mobile devices are concerned. Mobile devices should not be left unattended unless they are secured in some fashion, particularly when they are off campus.

It is the responsibility of staff to notify the Helpdesk at the earliest opportunity if an IT asset is lost, stolen or damaged. This is particularly important for mobile devices, where remote action will be taken to secure the information held on the device.

Mobile devices (smartphones / tablets, laptops) will have security management software installed. It is prohibited to remove this software, as it is essential to allow devices to be wiped of data in the event of loss or theft.

3.7. Staff Responsibility

It is the responsibility of all staff to ensure that no fixed IT hardware assets (desktops, Apple Macs, networked printers etc.) are moved from their established location or re- provisioned without the involvement of ITDS. No mobile device (laptop, tablet phone) should be redistributed without consultation with ITDS.

It is the responsibility of Line Managers to inform ITDS if the 'principal user' of a device has changed or a device is no longer in use or required e.g. in the event of staff leaving the institution. Arrangements for its return to ITDS should be made via the Helpdesk.

All equipment must be securely wiped of data relating to previous use. This is in accordance with the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) where if penalised can have serious consequences for the University in terms of reputable damage and the penalty of a substantial fine placed by the Information Commissioner's Office (ICO).

Following data erasure, all IT assets will be stored by ITDS in preparation for any future use request.

3.8. Compliance

Regular audits will be carried out by ITDS monitoring systems to ensure that assets are not being moved or transferred.

ITDS will also monitor usage of all networked PCs, laptops etc. and will recover assets for redeployment or disposal where there is no evidence of use for a continuous period of 6 months. Devices, which are not networked, will be subject to regular audits to ensure the device location and user is verified, and to ensure that any essential software updates and maintenance programme has taken place.

All staff must comply with the audit process by making hardware available for inspection when requested to do so.

Staff and visitors have a responsibility to ensure that they comply with this statement and its associated procedures. Failure to comply with any aspect of this statement will be dealt with in accordance with the University Disciplinary Procedure for staff.