UNIVERSITY OF SUSSEX

IT Asset Management Policy

Contents

Document Information

Document Title	**IT Asset Management Policy**
Release Date	21 January 2016
Version Number	1.0
Document Owner	Head of Service Delivery
Author	Peter Collier
Document Approval	IT Management Team
Approval Date	21 January 2016
Review Plan	To be reviewed annually

UNIVERSITY OF SUSSEX

1. Introduction

The University of Sussex has made, and continues to make, considerable investment into the IT infrastructure and systems (IT assets) that are used by students, staff, researchers and academics. These IT assets hold and manipulate important information, sometimes including information of a personal and sensitive nature.

It is therefore important that all IT assets, whether software or hardware, are appropriately managed from point of acquisition to time of disposal to ensure that IT assets deliver best value for the investment and appropriately protect the information that passes through them.

2. Purpose of this Document

This asset management policy provides the overall framework for the management of IT equipment from acquisition to disposal. This policy draws from the Financial Regulations and Information Security Policy.

It defines roles and responsibilities that relate to the implementation of this policy.

3. Scope

This policy applies to all staff, students and other members of the University who hold IT equipment purchased by the University.

(Note: Financial Regulations stipulate that all IT equipment must be purchased through IT Services with limited exceptions.)

IT equipment is currently defined as:

(a) All desktop, laptop and server computers and associated infrastructure;
(b) All monitors, printers and scanners;
(c) All phones, mobile and smartphones and portable computing equipment;
(d) Lecture Theatre and General Teaching Space equipment (projectors, microphones, cameras etc.);
(e) Routers, firewalls, switches, access points and other network infrastructure;
(f) Software licenses;
(g) Any other IT peripheral costing £100 or more.

As IT is by nature constantly changing, other items not listed here may still be required to be included in the asset management processes.

This policy also applies to all IT equipment forming part of the University's IT infrastructure (servers, network switches etc.) and equipment installed in teaching and research spaces, and open access areas.

4. Policy

The University of Sussex is committed to managing the lifecycle of its IT assets and everyone has a duty of care to protect IT assets at all time whether they are in use, storage, movement or in disposal.

IT assets shall be protected against physical or financial loss whether by theft, mis-handling or accidental damage either through primary prevention (e.g. physical security) or remediation (e.g. marking).

The University is committed to legal compliance in all regards of use and handling of IT assets.

All IT assets shall be traceable and auditable throughout the entire lifecycle.

Information about all IT assets shall be held in a suitable electronic database that enables them to be tracked, managed and audited throughout the entire lifecycle.

This policy shall be reviewed and updated on a regular basis to ensure that it remains appropriate due to the consequences of any relevant changes to the law, organisational policies or contractual obligations by IT Services Management Team.

5. Responsibility

Director of IT Services

The Director of IT Services is accountable for the implementation of this policy in the University. Responsibility of the day-to-day operation is normally delegated to the ITS Managers.

ITS Managers

All ITS Managers have responsibility for (delegating where appropriate):

a. Coordinating the audit of the equipment their team supports;

b. Updating and maintaining the accuracy of the inventory (such as equipment moves);

c. Ensuring that equipment is signed for (without amendment) by equipment holders and declaration is scanned into the asset management system;

d. Applying IT supplied barcode asset tag before equipment is taken out of IT Services care;

e. Checking equipment is returned in the same configuration as expected and signing pro-forma receipts upon collection from equipment holders;

f. Care of IT equipment held in stock for issuing and awaiting transfer for disposal;

g. Provide reports on any assets stripped for spares to the Departmental Manager and note components removed within the asset management system. Data on harvested drives will immediately have data destructed using a method approved by the Information Security Manager;

h. Printing and issuing replacement asset and location bar codes.

Head of IT Service Delivery

The Head of IT Service Delivery has responsibility for (and delegating where appropriate):

a. Ensuring that on collection new equipment is signed for by IT staff. IT equipment will not be issued by the purchasing team to porters or end users.

b. Issuing and fixing asset tags for IT equipment purchased through IT Services;

c. Entering Purchasing information on the asset management system;

d. Care for and security of equipment once transferred from technical and support teams for disposal;

e. Creating an asset list prior to disposal agents collection;

f. Confirming asset disposal on system using disposal reports.

IT Service Centre Manager and the Head of Student Desktop and AV Support

The Service Centre Manager and the Head of SDAVS have responsibility for:

a. Marking equipment as lost or stolen from the asset register;

b. Creating management reports including the annual audit report for the Director of Finance;

c. Adding IT equipment not purchased through IT Services where an exception under the Finance Regulations has been agreed in advance.

d. Ensuring the correct adherence to this policy by team members at all times.

Heads of Schools and Directors of Professional Services

Members of the School issued with IT equipment have the following responsibilities for the equipment in their care:

a. Loss or theft of IT equipment must be reported immediately to the Head of Security, Information Security Manager and the User Support Manager or IT Services Departmental Manager;

b. All IT equipment (including home working) must be returned to the relevant IT support team upon replacement, equipment redundancy (i.e. no longer required for University business) or when the holder or School severs affiliation. Equipment holders will retain responsibility for equipment issued to them until it has been returned to IT Services for redeployment or disposal;

c. Equipment holders are not permitted to transfer their responsibilities to another member of the School without the joint consent of the budget holder and the IT support team. Fixed IT equipment must not be moved without the consultation of IT Services and an update of asset data must be made;

d. Equipment holders must present mobile assets such as laptops and mobile phones to their support team for auditing within 2 weeks of request. Equipment may be presented for auditing at any time, but all equipment must be accounted for within a year of issuing or last being audited;

e. Equipment used for home working will be normally audited remotely. If equipment does not allow this alternative arrangements will be made.

f. IT equipment holders must make every effort to ensure that the equipment barcode asset marking is not damaged or destroyed whilst in their care;

g. In the event that a bar code asset marking has been damaged or destroyed the equipment holder must contact the appropriate support team immediately to arrange for a replacement marking;

h. Return equipment immediately that is not operating normally to their support team.

Staff and Representatives of IT Services

All IT Services staff and associated representatives must also ensure that they follow this policy, including:

a. Ensuring that any IT asset that is retired is disposed of in the correct way.

b. Updating asset registers correctly and as soon as a change is made.

c. Giving correct and appropriate advice to users and Heads of Schools on the correct handling of IT assets.

d. That any incorrect disposal or misuse of an IT asset is reported to an appropriate manager within IT Services as soon as possible.

6. Compliance

Any actual or suspected breach of this policy must be reported to the Head of IT Service Delivery, who will take appropriate action and inform the relevant internal and external authorities.

Failure to comply with this policy or the Financial Regulations may result in disciplinary action in accordance with the relevant process.

7. Revision history

Name	Date	Vers.	Change
Pete Collier	21/01/2016	1.0	Release version.