UNIVERSITY OF SUSSEX

IT Services

IT ASSET MANAGEMENT POLICY

1. OVERVIEW AND PURPOSE

1.1. The University of Sussex makes considerable investment into the IT infrastructure and systems (IT assets) that are used by students, staff, researchers and academics. These IT assets hold and process important information, including information of a personal and sensitive nature.

1.2. 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.

1.3. The purpose of this policy is to provide the framework for managing IT equipment from acquisition to disposal. This document also defines the roles and responsibilities that relate to the implementation of this policy.

2. SCOPE

2.1. This policy applies to all purchases of IT goods and services by the University and its subsidiary undertakings and joint ventures, except where the University's Audit and Risk Committee has approved an alternative policy for a specific subsidiary undertaking or joint venture.

2.2. It applies irrespective of the source of funding for a purchase and to purchases undertaken by all members of staff in connection with their University duties. Members of staff includes staff and any other individual authorised to undertake purchasing activity on behalf of the University.

2.3. Financial Regulations stipulate that all IT assets must be purchased through an approved supplier - IT Services is the approved supplier for the University of Sussex with limited exceptions.

2.4. IT equipment is currently defined as:

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

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

2.5. 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.

3. RESPONSIBILITIES

3.1. Director of IT Services

3.1.1. 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 IT Services Managers.

3.2. IT Services Managers

3.2.1. All IT Service Managers have responsibility for (delegating where appropriate):

- Auditing and maintaining an asset register of the equipment their team support.
- Updating and maintaining the accuracy of the inventory (such as equipment moves);
- Ensuring that equipment is signed for (without amendment) by equipment holders and declaration is scanned into the asset management system.
- Applying IT supplied barcode asset tag before equipment is taken out of IT Services care
- Installing any required discovery, reporting or management systems on all computers, mobile devices and servers before putting these items into service.
- Checking equipment is returned in the same configuration as expected and signing pro-forma receipts upon collection from equipment holders.
- Care of IT equipment held in stock for issuing and awaiting transfer for disposal.
- 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 must immediately have data destroyed using a method approved by the Cyber Security Manager.
- Printing and issuing replacement asset and location bar codes.

3.3. Deputy Director ITS Operations and Research

3.3.1. The Deputy Director ITS Operations and Research has responsibility for (and delegating where appropriate):

- 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.
- Issuing and fixing asset tags for IT equipment purchased through IT Services.
- Entering Purchasing information on the asset management system.
- Care for and security of equipment once transferred from technical and support teams for disposal.

- Creating an asset list prior to disposal agent's collection.
- Confirming asset disposal on system using disposal reports.

3.4. **Head of Service Operations and Change Management and Head of Technical Operations**

3.4.1. The Head of Service Operations and Change Management and Head of Technical Operations has responsibility for (and delegating where appropriate):

- Marking equipment as lost or stolen from the asset register.
- Creating management reports including the annual audit report for the Director of Finance.
- Adding IT equipment not purchased through IT Services where an exception under the Finance Regulations has been agreed in advance.
- Ensuring the correct adherence to this policy by team members at all times.

3.5. **Heads of Schools and Directors of Professional Services**

3.5.1. Heads of Schools and Directors of Professional Services issued with IT equipment have the following responsibilities for the equipment in their care:

- Loss or theft of IT equipment must be reported immediately to the IT Service Desk.
- To ensure that no arrangements or agreements are made to transfer University of Sussex IT equipment to individuals, for example when they leave the University's employment.
- 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 University severs affiliation. Equipment holders will retain responsibility for equipment issued to them until it has been returned to IT Services.
- IT equipment must not be moved or transferred to another person without the consultation of IT Services and an update of asset data must be made.

3.6. **Equipment Holders**

3.6.1. Equipment Holders issued with IT equipment have the following responsibilities for the equipment in their care:

- Ensure equipment is protected by a password which is compliant with the Account Management and Password Policy and take all reasonable steps to ensure that the password remains secret and known only to them.
- Not permit any unauthorised users, including members of their family or members of their household to use any UoS IT equipment, or access to their personal account.
- Be mindful of the placement of IT equipment, position screens appropriately to avoid being overlooked by those without permission to view the data.
- Always lock the screen when not in use and ensure device auto lock is enabled after ten minutes of inactivity.

- Ensure that University computer equipment (including mobile devices) is physically secured if left unattended.
- Keep any two-factor authentication token (if used) separate from the computer equipment.
- Report all losses/thefts of University equipment to their line manager and the IT Service Desk immediately.
- Make available IT equipment to the support team within the period stated on the communications.
- Make every effort to ensure that the equipment barcode asset marking is not damaged or destroyed whilst in their care.
- In the event that a bar code asset marking has been damaged or destroyed contact the IT Service Desk immediately to arrange for a replacement marking.
- Never attempt to disable anti-virus or end-point protection or any security software.
- Report any suspected malware outbreak or compromise to the IT Service Desk immediately.
- If using UoS equipment outside of the UK refer to Travelling Abroad with University Information Guidance (ISG02).
- Not make amendments to the core build of any UoS issued device, for example rebuilding, wiping or 'jailbreaking'.

3.7. **Staff and Representatives of IT Services**

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

- Be familiar with and understand this policy and any associated procedures.
- Ensuring that any IT asset that is retired is disposed according to the IT procedures.
- Updating asset registers correctly and as soon as a change is made.
- Giving correct and appropriate advice to users and Heads of Schools / Directors of Professional Service on the correct handling of IT assets.
- That any incorrect disposal or misuse of an IT asset is reported to IT Service Desk as soon as possible.

4. POLICY

4.1. 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 times whether they are in use, storage, movement or in disposal.

4.2. All IT assets have a finite lifespan, generally determined by availability of support and security updates. IT assets should be withdrawn from use when no longer fit for purpose, and will be securely wiped and disposed of through procedures determined by IT Services.

4.3. 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).

4.4. 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.

4.5. 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.

4.6. 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.

4.7. **Breach of Policy**

4.7.1. Any actual or suspected breach of this policy must be reported to the Deputy Director ITS Operations and Research who will take appropriate action and inform the relevant internal and external authorities.

4.7.2. Where there is deliberate misconduct or behaviour amounting to a wilful breach of this policy, or gross negligence causing a breach of the policy, the matter may be considered under the University's Disciplinary Procedure under Regulation 31.

5. LEGISLATION AND GOOD PRACTICE

5.1. The National Cyber Security Centre (NCSC) have issued guidance about secure sanitisation of data. https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media

5.2. The Payment Card Industry Data Security Standard has requirements regarding the management of IT Assets. https://www.pcisecuritystandards.org/pdfs/pci_ssc_quick_guide.pdf

5.3. Cyber Essentials helps to guard against the most common cyber threats and demonstrate commitment to cyber security. The requirements include the management of IT Assets.
https://www.ncsc.gov.uk/cyberessentials/overview
https://iasme.co.uk/cyber-essentials/

5.4. Asset Disposal and Information Security Alliance (ADISA) is an industry accreditation scheme for companies who provide IT Asset Disposal services and offers product approvals for companies with products which sanitise data.

5.5. All organisations that have access to NHS patient data and systems must use the Data Security and Protection Toolkit to provide assurance that they are practising good data security.
https://www.dsptoolkit.nhs.uk/

5.6. Electrical and electronic equipment (EEE) is regulated to reduce the amount of waste electrical and electronic equipment (WEEE) incinerated or sent to landfill sites. Reduction is achieved through various measures which encourage the recovery, reuse and recycling of products and components. The Waste Electrical and Electronic Equipment Regulations 2013 (as amended) is the underpinning UK legislation.
https://www.gov.uk/electricalwaste-producer-supplier-responsibilities
https://www.gov.uk/guidance/regulations-waste-electrical-and-electronic-equipment
https://www.hse.gov.uk/waste/waste-electrical.htm

Review / Contacts / References	
Policy title:	IT Asset Management Policy
Date approved:	13 October 2020
Approving body:	Information Governance Committee
Last review date:	December 2019
Revision history:	1.0 – 21 January 2016 2.0 - December 2019
Next review date:	October 2021
Related internal policies, procedures, guidance:	Information Security Policies Information Security Policy ITS Top 10 Security Tips Data Protection Payment Card Industry Data Security Standard Policy Financial Regulations Procurement and Purchasing Policy Purchasing Goods and Services Guide Waste and Recycling Travelling abroad with University information Guidance
Policy owner:	IT Services
Lead contact / author:	Pete Collier, Assistant Director, Strategy & Architecture (ITS)