Hardware Asset Management Policy

Version 1.0

Effective Date Immediate

HARDWARE ASSET MANAGEMENT POLICY
[v0.1]

Policies superseded by this version

This document replaces the Legacy Hardware Asset Policy of City, University of London, with effect from [*date*].

Summary of changes to previous version

The policy has been *re-written* following a review due to the merger of City University of London and St George's University of London.

Table of contents

1 Introduction

1.1 City St George's, University of London (the University) provides IT hardware to support teaching, research and professional services. Hardware assets represent a significant financial investment and, where they store or process University data, a material information security risk. Following the merger of City, University of London and St George's, University of London, a single approach to hardware asset management is required across the whole institution.

This policy forms part of the University's Information Security Management System (ISMS), which is aligned to ISO/IEC 27001:2022. It should be read alongside the Acceptable Use Policy, the BYOD Policy and the Data Protection Policy.

2 Freedom of Speech and Academic Freedom

2.1 City St George's, University of London, regards freedom of speech and academic freedom to be fundamental to delivering its mission as the University of business, practice and the professions. Its values in this respect are set out in a code of practice on freedom of speech and academic freedom, which explains how the University will uphold, secure, and promote freedom of speech within the law: https://www.citystgeorges.ac.uk/about/governance/policies/code-of-practice-on-freedom-of-speech.

2.2 Nothing in this policy should be interpreted in any way that would be inconsistent with the code of practice and – in the event of any inconsistency – the provisions of the code will prevail.

2.3 The Office for Students ("OfS") operates a free speech complaints scheme. Under that scheme, the OfS can review complaints about free speech from non-student members, staff, applicants for academic posts and (actual or invited) visiting speakers. The scheme is free to use. Information about the complaints that the OfS can review is available on its website at: www.officeforstudents.org.uk/for-providers/freedom-of-speech/free-speech-complaints. Student complaints about freedom of speech issues are handled by the Office of the Independent Adjudicator for Higher Education ("OIA"). Information about how the OIA handles such complaints can be found on its website (https://www.oiahe.org.uk/resources-and-publications/latest-news-and-updates/oia-highlights-role-in-student-free-speech-complaints/).

3 Equity, Diversity and Inclusion

3.1 City St George's, University of London works to advance equity, diversity and inclusion in its activities, processes, and culture, for the whole University community, including staff, students and visitors.

3.2 The University will meet its obligations under the Equality Act 2010 in its policies and seek to eliminate discrimination on the basis of age, caring responsibilities, disability, gender identity, gender reassignment, marital status, neurodiversity, pregnancy, race, religion or belief, sex, sexual orientation, and socio-economic background.

4 Definitions

4.1 **Hardware asset** – Any physical IT equipment owned, leased or managed by the University, including desktops, laptops, tablets, monitors, docking stations, servers, network equipment and peripherals.

4.2 **Managed device** – A hardware asset that is enrolled in the University's endpoint management platform and subject to centrally managed security controls, encryption and software deployment.

4.3 **Standard device** – The default hardware specification approved by IT for general use. Current specifications are published in the IT Product Catalogue.

4.4 **Non-standard device** – Any hardware that differs from the standard specification, including alternative operating systems, specialist research equipment or devices from non-approved suppliers.

4.5 **Asset register** – The University's central record of all IT hardware assets, recording the full lifecycle of each asset from procurement through to disposal.

4.6 **Secure disposal** – The process of permanently and irreversibly removing all data from a device before it is recycled or destroyed, in accordance with University procedures and applicable environmental regulations.

4.7 **Security exception** – A formal, time-limited approval to deviate from the standard security controls, granted following a documented risk assessment and business justification.

5 Policy

5.1 Procurement

All IT hardware must be purchased through IT, irrespective of the funding source. This includes equipment funded from departmental budgets, research grants, charitable funds or any other source. Hardware procured outside IT will not be supported, connected to the University network or recorded in the asset register.

IT will procure hardware from approved suppliers in accordance with the University's procurement regulations. Requests for non-standard hardware must include a business justification and the approval of the relevant head of department or dean.

5.2 Ownership and asset registration

All IT hardware procured by or on behalf of the University is and remains the property of the University, regardless of the funding source.

All hardware assets must be recorded in the University's asset register. The register must record the full lifecycle of each asset, including asset type, serial number, date of procurement, assigned user, location, warranty status, any transfers or reassignments and the date and method of disposal. The asset register will be maintained by IT and reviewed periodically to ensure accuracy.

5.3 Standard allocation

Each member of staff is allocated a single laptop as standard, provided to the University's current standard specification. A desktop may be requested as an alternative where the individual does not take advantage of hybrid working arrangements.

Where a laptop is allocated, IT will also provide a docking station, monitor, keyboard and mouse to support office-based working. Standard devices will be within their warranty period and will run the University's managed operating system build.

Students are not provided with personal IT equipment. Students should make use of the University's student computing labs, library facilities and open-access workstations. Where a student participates as a member of a funded research project that requires dedicated equipment, the project sponsor may provide a device funded by the project budget. The project sponsor is accountable for the equipment and must ensure it is recorded in the asset register, subject to University security controls and returned to IT at the end of the project or the student's affiliation.

5.4 Security requirements

All University hardware assets must comply with the following security requirements. It is expected that allocated devices will be in regular use, as this is necessary to receive security patches, operating system updates and policy changes. Devices that remain disconnected for an extended period may be disabled or quarantined.

- Full disk encryption must be enabled on all laptops and portable devices. Encryption must not be removed or disabled.
- Devices must run the University's managed build, including centrally deployed anti-malware, firewall and endpoint detection and response software.
- Users must not disable, remove or alter security controls on University devices, including encryption, anti-malware, screen locks or endpoint management agents.
- Users must not install software, operating system components or drivers on managed devices without authorisation through the IT Service Desk or a security exception.
- Devices must be physically secured when unattended. Laptops and portable devices must not be left unsecured in public or shared spaces.

Where a user has a legitimate business need for elevated privileges, augmented technical controls or a deviation from the standard security configuration, they may apply for a security exception. Requests must be submitted to the Information Security Manager with a documented business justification and will be subject to a risk assessment. Approved exceptions are time-limited and subject to periodic review.

5.5 Loss, theft and damage

Users must report the loss, theft or damage of any University hardware asset to the IT Service Desk immediately. In the case of theft, users must also report the incident to the police and provide IT with the crime reference number. Where a lost or stolen device may hold personal data or sensitive information, the incident will be assessed by the Information Assurance Team alongside IT to determine the risk and whether notification to the Information Commissioner's Office or affected individuals is required under the UK GDPR.

Users may be held responsible for damage caused by negligence or misuse. The University reserves the right to recover reasonable costs in such circumstances.

5.6 Return and transfer of assets

All University hardware must be returned to IT when no longer required, when the user's role changes or when the user's affiliation with the University ends. The user's line manager is accountable for ensuring that hardware is returned as part of the leaver or transfer process.

University hardware must not be retained for personal use, sold, gifted or disposed of by the user. Devices can only be repurposed or reassigned by IT.

5.7 Secure disposal

Before any University hardware is disposed of, sent for repair or transferred to another user, all data must be securely erased in accordance with the University's procedures. Secure erasure must meet or exceed the standards set out in NCSC guidance on secure sanitisation.

The University does not sell, donate or gift IT equipment to staff, students or third parties. All end-of-life hardware must be disposed of through IT in accordance with applicable environmental regulations, including the Waste Electrical and Electronic Equipment (WEEE) Regulations. IT will maintain records of all asset disposals, including the method of data destruction, for audit purposes.

5.8 Warranty and replacement cycle

Standard devices are replaced cyclically at the end of their warranty period. Devices that are out of warranty remain the property of the University and will be replaced through the standard process. Users should request a replacement via the IT Service Desk.

Users must respond promptly to IT requests to return or replace hardware. Devices that have reached end of life or are no longer supported may develop security vulnerabilities that place University data and systems at risk. Where a user fails to respond to replacement requests within a reasonable timeframe, IT reserves the right to disable or quarantine the device to protect the University's network and information assets.

Peripheral devices such as monitors, docking stations and keyboards are replaced on failure. These items are not part of the standard replacement cycle.

5.9 Purpose

The purpose of this policy is to ensure that all IT hardware owned, leased or managed by the University is procured, recorded, allocated, secured, maintained and disposed of in a controlled and consistent way. It establishes that all hardware, regardless of funding source, remains University property and is subject to the University's managed security controls, and it defines the obligations of IT, line managers and users throughout the asset lifecycle. In doing so, the policy protects University information, supports operational continuity, ensures an accurate and auditable asset register, and enables the University to meet its legal, regulatory and contractual obligations, including UK GDPR and the WEEE Regulations.

5.10 Scope

This policy applies to all IT hardware assets owned, leased or managed by the University, regardless of how they were funded. This includes equipment purchased from departmental budgets, research grants or central IT budgets.

This policy applies to all staff, contractors and any other persons to whom University hardware is issued. It covers the full lifecycle of hardware assets from procurement and allocation through to return, repurposing and disposal. Personal devices may only be used in accordance with the BYOD Policy.

5.11 Principles

This policy sets out the principles governing the procurement, allocation, management, security and disposal of University-owned IT hardware. It ensures that hardware assets are recorded, protected, maintained and disposed of in a manner that safeguards information, supports operational continuity and meets the University's legal, regulatory and contractual obligations.

5.12 Roles and responsibilities

a. Chief Information Officer (CIO)

Accountable for the University's hardware asset management strategy and for ensuring that appropriate controls are in place to protect hardware assets throughout their lifecycle.

b. IT department

Responsible for procuring, configuring, deploying, maintaining, tracking and disposing of University hardware in accordance with this policy. IT maintains the asset register and ensures that all devices meet the University's security standards before deployment.

c. Information Security Manager

Provides advice on the security requirements for hardware assets, conducts security assessments for non-standard device requests, manages the security exception process and oversees compliance with the security provisions of this policy.

d. Line managers and supervisors

Ensure that hardware is requested in a timely manner for new starters and that team members comply with this policy. Line managers are accountable for ensuring that all University hardware is returned as part of the leaver or transfer process and must confirm with IT that assets have been received.

e. All users

Responsible for the care, physical security and proper use of University hardware allocated to them. Users must comply with all security requirements, report loss, theft or damage immediately (including reporting theft to the police and providing a crime reference number) and return hardware when it is no longer required or when their affiliation with the University ends.

f. Research supervisors and project sponsors

Responsible for ensuring that hardware requests for research students are properly justified, funded and procured through IT. Project sponsors are accountable for equipment provided to students and must ensure it is recorded in the asset register, subject to University security controls and returned to IT at the end of the project.

6 Procedure

6.1 Requesting hardware

All hardware requests must be submitted through the IT Service Desk or the IT self-service portal. For new starters, IT must be notified at least two weeks before the agreed start date. Requests for non-standard equipment must include a business justification and the appropriate approval. Where non-standard equipment is approved, delivery times may vary.

6.2 Device build and deployment

All devices will be configured with the University's managed build, including the standard operating system, productivity software, security controls and endpoint management. Users requiring specialist software must specify this at the time of request. Software will be installed only where the University holds a valid licence.

6.3 Security exceptions

Users who require elevated privileges, additional software or modifications to the standard security configuration must apply for a security exception through the Information Security Manager. Requests must include a business

justification and will be assessed against the risk to the University. Approved exceptions are time-limited and recorded in the exceptions register. The Information Security Manager will report active exceptions to the IGSC.

6.4 Asset tracking

IT will record all hardware assets in the asset register at the point of deployment and update the register throughout the asset's lifecycle as it is transferred, returned, repurposed or disposed of. The asset register will be audited periodically against physical inventory.

6.5 Leaver and role-change process

Line managers must notify IT when a member of staff or contractor is leaving or changing role. The line manager is accountable for ensuring that hardware is returned. IT will arrange for data to be securely erased and the asset register to be updated. Users must not retain University hardware beyond the end of their affiliation.

7 Monitoring

Compliance with this policy will be monitored through the asset register, endpoint management reporting, periodic audits and the University's information security assurance activities. Non-compliance may be identified through audit, incident investigation or management review.

8 Advice and guidance

8.1 IT Service Desk

The first point of contact for hardware requests, faults, replacements and queries about this policy.

8.2 Information Security Manager

Provides advice on security requirements for hardware, non-standard device assessments, security exceptions and compliance.

8.3 IT Product Catalogue

Current standard device specifications and approved hardware options are published in the IT Product Catalogue, available via the IT self-service portal.

Users are encouraged to contact the IT Service Desk if they are uncertain about any aspect of hardware procurement, allocation, security or return.

9 Failure to comply

9.1 Users

Failure to comply with this policy may result in withdrawal of access to University systems, mandatory retraining or other corrective measures. Serious or repeated breaches, including failure to return hardware, procurement of hardware outside IT, or deliberate circumvention of security controls, may lead to disciplinary action under the relevant University procedures. Users may be held responsible for costs arising from negligence or misuse.

9.2 Legal and regulatory obligations

Where a breach involves personal data, security-sensitive materials or other unlawful activity, it may be reported to external authorities including the Information Commissioner's Office or law enforcement.

9.3 Academic freedom and lawful expression

Actions taken under this policy will be applied consistently with the University's duties under the Higher Education (Freedom of Speech) Act 2023. Disciplinary or corrective measures will not be imposed for lawful academic expression or research activity.

10 Review

This policy shall be reviewed at least annually or following significant changes in technology, procurement arrangements or organisational structure. Updates require approval by the Information Governance and Security Committee.

Normative references

- ISO/IEC 27001:2022 Annex A controls A.5.9, A.5.11, A.7.9, A.7.10, A.7.13, A.7.14, A.8.1
- NIST Cybersecurity Framework
- Cyber Essentials technical requirements
- NCSC guidance on secure sanitisation of storage media
- Waste Electrical and Electronic Equipment (WEEE) Regulations 2013
- UK GDPR and Data Protection Act 2018

This policy forms part of the University's ISMS suite governed by the Information Security Policy.

Policy information

Should you require further information regarding this policy or access to the policy in an alternative format, then please contact the *CIO, cio-office@citystgeorges.ac.uk*.

Policy Title:	Hardware Asset Management Policy
Policy Version:	V 1.0
Primary Author:	Eric McIntosh
Related Policies:	
Accountable Authority:	Chief Digital Information Officer
Approving Authority:	Information Governance and Security Committee
Date of Approval:	June 2026
Policy effective from:	Immediate
Date of Review:	June 2027

Appendix

[*An appendix to a policy may be used to set out specific procedures, contact information, examples of how to comply, etc*]