Imperial College
London

Imperial College

Code of Practice 1: Hardware and Software Asset Management

Doc. Ref.	: Code of Practice 1: Hardware and Software Asset Management
Version	: 2.0
Status	: Approved
Date	: 28/03/2022
Approved by	: The Information Governance Steering Group
Review by	: 28/03/2024

INTRODUCTION

Definition and Objective

This code of practice defined how the College meets its legal and contractual obligations through the purchase, usage, licensing and management of Information Technology (IT) hardware and software. Please see the "Scope" section for a full definition of IT hardware and software.

In so doing the College can remain compliant with the agreements it enters into with suppliers and help ensure value for money for the organisation.

It should be read in conjunction with the College's Information Security Policy and, in particular, Section 11 regarding the Conditions of Use of IT Resources.

Scope

This policy applies to all staff and students involved in the specification, acquisition, installation, use and maintenance of IT hardware and software, whether it is purchased outright, renewed, leased, or hosted via a third party, e.g. software as a Service (SaaS), shareware or freeware.

Hardware: IT equipment including PCs (desktop computers), including all-in-one desktop machines such as iMacs, laptops, servers, tablets, other mobile handheld devices including mobile phones, storage devices and Audio Visual equipment (video screens, projectors and AV consoles) purchased directly by the College, or through research grants are included in the scope of the CoP. Peripheral devices such as standard display units, docking stations, keyboards, mice, USB storage devices, etc. are excluded.

Software: All College software, whether purchased, leased, obtained under 'shareware', 'freeware' or trial arrangements, acquired under suppliers' educational support agreements, or developed in-house, and whether installed on-campus or off-campus are included. This covers all applications, add-ons and/or extensions to those applications and operating systems.

PRINCIPLES AND RESPONSIBILITIES

The College is the sole owner of all IT assets purchased using the College funds and College research grants. All devices are configured and managed by ICT to comply with information security and data protection requirements. This requires management software to be configured on these devices.

IT Hardware

All IT hardware assets must be recorded in the College's Asset Management System (AMS), with the following fields populated as a minimum: asset number, serial number, description, make and model, custodian and primary user.

Each IT hardware asset should be assigned a "custodian" at the point of purchase order approval, which should be kept up to date during its lifecycle until they have been disposed of properly. They are

accountable for the assets assuming their ownership on behalf of the College. Custodians must:

- Be current employees of the College on payroll.
- Check that all assets in scope are recorded in the College Asset Management System and are asset tagged.
- Allocate assets to primary users for their use.
- Inform primary users of their responsibilities, and most importantly that they should look after College assets properly.
- When leaving, or moving to another role within the College, ensure that the custodianship of assets are handed over to another College custodian. If this is not done, their line manager, by default, will be the next custodian.
- Ensure that the assets at the end of their lifecycle are disposed off properly. Failure to do so may be subject to College action.

"Primary users" are responsible for the assets: Primary users must:

- Be current staff or students of the College.
- Use their assets in line with the College's Conditions of Use of IT Resources.
- Protect their assets and ensure necessary precautions are taken at all times.
- When leaving, or moving to another role within the College, ensure that their assets are returned to the custodian.

All devices in scope should be assigned an eight-digit asset number and asset tagged using the College's standard asset tag shown below. Handheld devices may not be tagged with a physical asset tag for practical purposes, and will be assigned a virtual asset number starting with 9 in the AMS.

For practical reasons, devices with wireless capabilities can be self-registered for use on the College network by their users, thus potentially avoiding asset tagging and registration in the AMS. If an IT asset is purchased using College funds, it is the responsibility of the approver of the funds that they are registered in the AMS and are asset tagged. Self-registered devices can be declared to ICT Service Desk with the relevant purchase details. ICT will then assign an asset tag and register them on the AMS, updating their custodian and primary user.

IT Software

Software must be installed on College computers or networks only after appropriate licences have been acquired, and it's been confirmed that its use is in accordance with its licensing terms and conditions. These may include geographical restrictions, and apply to where software is accessed from rather than specifically where it is hosted.

Appropriate support and maintenance should always be included in software purchase agreements so that any software issues and/or security

vulnerabilities can be managed proactively and appropriately.

ICT will normally support the latest version of a software application plus its immediate predecessor. More versions may be supported provided an agreement is reached due to operational or any other issues. Any requests related to extended support or upgrades should be raised as a Service Desk ticket.

ICT install and use software management software on all ICT managed computers to diagnose and monitor software licensing and usage. This allows ICT to collect information about the use of software across all computers optimising the licence use and software costs.

ICT monitor and investigate software licence use and from time to time may have to take appropriate measures to maintain compliance. This may include requests for, or automated methods of uninstalling / deleting software which are not in accordance with the usage terms and conditions. These requests may also extend to personal devices accessing the College network.

PROCESS

Purchasing

College hardware and software must be purchased in accordance with the College's financial regulations and the purchasing guidance provided on College Purchasing pages.

If you are looking to purchase standard College hardware and software, information can be found on ICT's "Get Devices and Software" web page.

If you are looking to purchase non-standard hardware or software, or develop software for College use, you should contact the ICT Department by raising a Service Desk ticket to review the business need and all options available before starting to look into suppliers and making a decision to use a particular digital solution. If a decision is made in isolation and obligations are entered into without consulting with the College Purchasing and ICT first, it may not be possible for the College to fulfil those obligations.

Version History

Version/Status	Release Date	Comments
0.1/Draft	24/08/2020	Written based on the recommendations of the IT Equipment Lifecycle Group (2017) and ICT's Software Compliance Group (2020)
1.0/Approved	January 2021	Published linked to InfoSec Policy v6.0.
1.1/In Review	March 2022	"All devices are configured and managed by ICT to comply with information security and data protection requirements. This requires management software to be configured on these devices." added in paragraph 2.1.
2.0/Approved	March 2022	Published linked to the InfoSec Policy.