RCSI DEVELOPING HEALTHCARE LEADERS WHO MAKE A DIFFERENCE WORLDWIDE

RCSI IT Asset Management Policy

Policies and procedures | RCSI Staff Portal

RCSI

Document Control

Version	Date	Action	Author
0.1	03/2/2023	Draft Asset Management Policy	Ruth Meredith
1.0		Published RCSI IT Asset Management Policy	Ruth Meredith

Approver List

Name	Title	Dept	Approved Date
Justin Ralph	CIO	IT	03/02/2023
Ruth Meredith	IT SDM	IT	03/02/2023
Pat Barry	IT Infrastructure Manager	IT	03/02/2023

RCSI

Contents

1. Purpose

The Royal College of Surgeons Ireland (RCSI) is legally required to ensure the appropriate management of IT assets provided to and used by its students and employees.

The purpose of this policy is to maintain appropriate protection of organisational assets, and to avoid breaches of any criminal and civil law, statutory, regulatory, or contractual obligations. This Policy provides direction on the management of RCSI's IT assets.

This policy is mandatory and by accessing any Information Technology (IT) resources which are owned or leased by the RCSI, users are agreeing to abide by the terms of this policy.

2. Scope

This policy represents the RCSI's national position and takes precedence over all other relevant policies which are developed at a local level. The scope addresses the Asset Management policy. This policy should be/is compatible with, but does not supersede or guarantee compliance with all IE and EU standards

The policy applies to:

2.1. Physical and Virtual Assets

End user devices:

- Laptops, desktops, peripherals, etc.
- Other portable computing devices including smartphones and tablets.

Infrastructure:

- Servers
- Midrange/multiuser systems
- Storage devices e.g. Disk Arrays, Tape Libraries, etc.
- Network devices, e.g. routers, switches, APs, etc.

2.2. Software Assets

Software is included where it is installed on infrastructure components and is (or may be) separately licensed. This includes, but is not limited to, Operating systems, middleware, database, and application software.

2.3. Information Assets

RCSI's information assets include data such as student data, employee data, financial data, and research data which are important and critical to the University.

3. Policy

All assets will have an asset assignee. The asset assignee has overall responsibility for the integrity, availability, and protection of the asset. RCSI IT retains overall responsibility and ownership for all IT assets. Assignees of IT assets are responsible for the protection, integrity, and availability of those assets and for putting the appropriate controls and procedures in place.

3.1. Asset Life Cycle Asset Acquisition

- Assets covered under the scope above must be sourced via a RCSI approved supplier.
- University policy and local procurement guidelines must be followed. IT asset acquisitions requiring the support of RCSI IT must be agreed with RCSI IT prior to procurement.
- All purchase of new systems hardware / software or new components must be made in accordance with relevant Information Security and other University policies, as well as technical standards.

3.2. Installation

- All authorised equipment must be fully and comprehensively evaluated, tested, assessed for fitness of purpose, hardened to security standards, and formally accepted by the users before being transferred to the live environment.
- Hardening standards must be followed for all new hardware and software prior to production implementation.

3.3. Disposals and Recycling

- All data and configuration setting (including User Ids and passwords) must be permanently deleted prior to disposal.
- Computer Equipment must be disposed of in a safe and environmentally friendly manner, in accordance with local legal requirements (including copyright principles and licence terms).

3.4. Rights of Use – Software Licensing

- Approval of purchase and deployment of software licence agreements (Including EULAs/End User Licence Agreements) must only be done through approved processes.
- Purchasing documentation (including executed contracts) relating to software must be filed and retained in perpetuity to provide a historical record and evidence of prior licensing arrangements, including evidence of entitlement to current versions of software based on an upgrade path.
- Software licence certificates must be retained in a secure environment with limited and managed access controls.

3.5. Asset Register

- All assets covered under the scope above (owned and leased), excluding end user devices, must be captured on the appropriate Asset Register.
- All such assets must have an identified assignee, captured in the asset register, and be tracked throughout its lifecycle.
- Periodic checks of the hardware and software installed may take place to ensure that the asset register is an accurate reflection of the physical installations.
- Assets owned by the University may only be disposed of with the agreement of the IT Asset assignee.
- When such assets are disposed of, the Asset Register must be updated to show that IT equipment / hardware has been decommissioned and the method of its disposal (the asset must not simply be deleted from the register).

3.6. Disaster and Business Recovery

Assignees must be able to demonstrate that critical business applications that include licensed software are identified and that the licence permits use of that software at a different site, university location or computer, all of which may be operated by a third party.

4. Roles & Responsibilities

4.1. IT Department

The IT Department is responsible for:

- The management, control, ownership, security, and integrity of all RCSI's network domain (LAN/WAN) including email services, on behalf of RCSI.
- The implementation of this policy and all other relevant policies within the IT remit.
- Ensuring adequate procedures are in place to ensure compliance with this policy and all other relevant policies.
- Ensuring adequate technologies are in place to ensure compliance with this policy and all other relevant policies.

4.2. Department Heads and Line Managers

Each Manager is responsible for:

- The implementation of this policy and all other relevant RCSI policies within the business areas for which they are responsible.

- Ensuring that all members of staff who report to them are made aware of and are instructed to comply with this policy and all other relevant RCSI policies.

- Consulting with the HR, IT and DPO/Legal Department in relation to the appropriate procedures to follow when a breach of this policy has occurred.

4.3. Users

Each user is responsible for:

- Complying with the terms of this policy and all other relevant RCSI policies, procedures, regulations, and applicable legislation.

- Respecting and protecting the privacy and confidentiality of the information systems and network they access, and the information processed by those systems or networks.

- Complying with instructions RCSI IT by designated information owners, system administrators, network administrators and/or the IT Department on behalf of RCSI.

- Reporting all misuse and breaches of this policy to their Line Manager.

5. Enforcement

- The RCSI reserves the right to take such action, as it deems appropriate, against individuals who breach the conditions of this policy. RCSI staff, students, contractors, sub-contractors or agency staff that breach this policy may be subject to disciplinary action, including suspension and dismissal as provided for in the RCSI disciplinary procedure.

- Breaches of this policy by a third-party commercial service provider, may lead to the withdrawal of RCSI information technology resources to that third party commercial service provider and/or the cancellation of any contract(s) between the RCSI and the third-party commercial service provider.

- Where illegal activity is suspected RCSI may refer any use of its IT resources, without notice to the user of the resources, to the Gardaí.

6. Review & Update

- This policy will be reviewed and updated annually or more frequently if necessary to ensure any changes to the RCSI's organisation structure and business practices are properly reflected in the policy.

7. Supporting documents

- RCSI Information Security Policy
- RCSI IT Purchasing Policy
- RCSI IT Equipment Provisioning Policy
- Disposal of IT Equipment
- RCSI IT Sustainable IT Policy
- RCSI Data Protection Policies and Procedures