RCSI

RCSI DEVELOPING HEALTHCARE LEADERS WHO MAKE A DIFFERENCE WORLDWIDE

RCSI Internet Usage Policy

Document Location: http://staff.rcsi.ie/administration-and-support/information-technology/policies-and-procedures/

Document Control

Version	Date	Action	Author
0.1	11/06/2018	RCSI Internet Usage Policy	Ruth Meredith
1.0	31/07/2018	Published	Ruth Meredith
1.0	15/08/2018	Spelling error changed	Ruth Meredith
1.1	29/07/2021	Updated document title on title page. Updated Infrastructure Manager to Pat Barry Updated Purpose from employees to approved users. Updated Scope to include mobile device. Updated 5.3 to include additional approvers for non-CSIRT requests. Updated 5.5 to remove HR as approvers. Updated 5.6 to remove HR as approvers and add Department Heads as approvers.	Ruth Meredith
1.1	06/09/2021	Reviewed and resolved comments. Updated wording accordingly	06/09/2021

Reviewer List

Name	Title	Dept	Reviewed Date
Justin Ralph	Chief Technology Officer	I.T.	24/08/2021
Ruth Meredith	IT SDM	I.T.	29/07/2021
Pat Barry	IT Infrastructure Manager	I.T.	06/09/2021
Dónall King	Legal Counsel and DPO	Legal, DPO	24/08/2021

Approver List

Name	Title	Dept	Approved Date
Justin Ralph	Chief Technology Officer	I.T.	24/08/2021
Ruth Meredith	IT SDM	I.T.	06/09/2021
Pat Barry	IT Infrastructure Manager	I.T.	06/09/2021
Dónall King	Legal Counsel and Data Protection Officer	Legal, DPO	24/08/2021

Contents

1. Policy Statement

Information is a critical asset of The Royal College of Surgeons Ireland (“RCSI”). Accurate, timely, relevant, and properly protected information is essential to the success of RCSI's Academic and Administrative activities. RCSI is committed to ensuring all accesses to, uses of, and processing of College information is performed in a secure manner.

The object of this Internet Usage Policy is to define the security controls necessary to safeguard University Information Systems and ensure the security confidentiality and integrity of the information held therein.

2. Overview

Access to the Internet is provided for research, teaching, learning and other legitimate College related activities. Incidental and personal use of the Web is permitted as long as such use does not disrupt or distract the individual from College business (due to volume, frequency or time expended), does not incur unreasonable cost to RCSI, and/or does not restrict the use of those systems to other legitimate users.

3. Purpose

The purpose of this policy is to define standards for systems that monitor and limit web use from any host within the RCSI network. These standards are designed to ensure approved users use the internet in a safe and responsible manner, and ensure that web use can be monitored or researched during an incident.

4. Scope

This policy applies to all RCSI employees, students, contractors, vendors and agents with an RCSI-owned or personally owned computer, workstation or mobile devices connected to the RCSI network.

This policy applies to all end user initiated communications between RCSI’s network and the internet, including web browsing, instant messaging, file transfer, file sharing, and other standard and proprietary protocols. Server to Server communications, such as SMTP traffic, backups, automated data transfers or database communications are excluded from this policy.

This policy represents the RCSI’s national position and takes precedence over all other relevant policies which are developed at a local level.

5. Policy

5.1. Unacceptable Usage

The following list represents the main unacceptable usages for RCSI internet services. This list is not considered exhaustive and is intended to demonstrate the spirit of this policy:

- The pursuit of private commercial business activities or profit-making ventures (i.e., employees may not operate a business with the use of RCSI computers and Internet resources);
- Representation or commitment of RCSI to any contract or service without express written permission;
- Use of Internet sites that result in an additional charge to RCSI;
- Engaging in prohibited discriminatory conduct such as the obtaining, viewing or sharing of sexually explicit material;
- Any activity that would bring discredit on RCSI;
- Any use or activities which are disruptive to the work place or in violation of college trust;
- Use of RCSI resources to gain unauthorised access to any web site, network, or system. College resources may not be used to interfere with or affect the operation of RCSI or any other systems on the Internet;
- Invade the privacy of others;
- Make any attempt to damage computer equipment or software;
- Download of illegal, hacked or cracked software;
- Engage in any activity that is harassing or defamatory;
- Use the Internet for any illegal activity, including violation of copyright or other rights of third parties, or in a manner inconsistent with RCSIs business.

5.2. Website Monitoring

The Information Technology Department will monitor internet use from all computers and devices connected to the corporate network. For all traffic the monitoring system will record the source IP Address, the date, the time, the protocol, and the destination site or server. Where possible, the system will record the User ID of the person or account initiating the traffic. Internet Use records will be preserved for 6 weeks.

5.3. Access to website monitoring reports

General trending and activity reports can be made available as needed upon request to the Information Technology Department.

Computer Security Incident Response Team (CSIRT) members may access all reports and data if necessary to respond to a security incident. Internet Use reports that identify specific users, sites, teams, or devices will only be made available to associates outside the CSIRT upon written or email request to IT with approval from the Department Head and/or SMT member and HR for RCSI employees and students. Approval from the Department Head and/or SMT member and the CTO for non-RCSI employees, third parties, vendors etc.

5.4. Internet Use Filtering System

The Information Technology Department will block access to Internet websites and protocols that are deemed inappropriate for RCSI's environment. The following protocols and categories of websites should be blocked:

- Adult/Sexually Explicit Material;
- Advertisements & Pop-Ups;
- Gambling;
- Hacking;
- Illegal Drugs;
- Peer to Peer File Sharing;
- SPAM, Phishing and Fraud;
- Spyware;
- Tasteless and Offensive Content;
- Violence, Intolerance and Hate.

5.5. Internet Use Filtering Rule Changes

The Information Technology Department will periodically review and recommend changes to web and protocol filtering rules. Changes to web and protocol filtering rules will be recorded as part of the CAB process.

5.6. Internet Use Filtering Rule Exceptions

If a site is miscategorised, employees may request the site be unblocked by submitting a ticket to the IT Helpdesk. IT will review the request and unblock the site if it is miscategorised.

Employees may access blocked sites with permission if appropriate and necessary for business purposes. If an employee needs access to a site that is blocked and appropriately categorised, they must submit a request to their Department Head. Their Department Head will request approved exception requests to Information Technology by IT Portal ticket or by email. Information Technology will unblock that site or category for that associate only. Information Technology will track approved exceptions and report on them upon request.

6. Management Roles & Responsibilities

6.1. The Senior Management Team (SMT)

The SMT is responsible for distributing the IT Information Security Policy to all heads of Departments/Schools/Faculties/Research and for supporting the Chief Technology Officer in the enforcement of the policies where necessary.

6.2. Department Heads of Academic, Research and Administrative Areas

Heads of Academic, Research and Administrative areas are required to familiarise themselves with the policies.

Heads of Academic, Research and Administrative areas are obliged to ensure that all IT systems under their remit are formally administered either by an administrator appointed by the head of an Academic, Research and Administrative areas or centrally by IT. The duties of the administrator are set out in the associated supporting policy.

- The implementation of this policy and all other relevant policies within the RCSI Department or service they manage;
- Making sure adequate procedures are implemented within their Department or service, so as to ensure all RCSI employees, third parties and others that report to them are made aware of, and are instructed to comply with this policy and all other relevant policies;
- Notifying the appropriate resources, if they suspect a user is responsible for misusing the information system or is in breach of this policy;
- Informing the appropriate resources immediately in the event of a security incident, including suspected data breaches, involving the system or data they are responsible for;
- Complying with instructions issued by the CTO on behalf of the RCSI.

6.3. Line Managers

Each Line 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, Legal and Data Protection Department in relation to the appropriate procedures to follow when a breach of this policy has occurred.

6.4. 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 issued by designated information owners, system administrators, network administrators and/or the I.T. Department on behalf of the RCSI;

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

6.5. I.T. Department

The I.T. Department is responsible for:

- The management, control, ownership, security and integrity of all RCSI network domain (LAN/WAN/Wi-Fi) on behalf of the RCSI;

- The implementation of this policy and all other relevant policies within the I.T. 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;

- Providing information owners or their nominees with audit reports and user access lists for information systems which are directly managed by the I.T. Department.

7. Breaches of Security

7.1. Incident Reporting

Any individual suspecting that there has been, or is likely to be, a breach of information systems security should inform the IT Security Officer (or equivalent) or the CTO immediately who will advise RCSI on what action should be taken.

7.2. 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 breaches this policy may be subject to disciplinary action, including suspension and dismissal as provided for in the RCSI disciplinary procedure.

The RCSI may refer any use of its I.T. resources for illegal activities to the Gardaí.

7.3. Legal Implications

Any breach of security of an Information System could lead to loss of security of personal information. This would be an infringement of the General Data Protection Regulations and could lead to civil or criminal proceedings. It is vital, therefore, that users of RCSIs Information. Systems must comply, not only with this policy, but also with the College's Data Protection policies.

8. 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.

Appendix A

- **Authorisation / Authorised:** Official RCSI approval and permission to perform a particular task.
- **Backup:** The process of taking copies of important files and other information stored on a computer to ensure they will be preserved in case of equipment failure or loss/theft etc.
- **Confidential information:** Information which is protected by Irish and/or E.U. legislation or regulations, RCSI policies or legal contracts. The unauthorised or accidental disclosure of this information could adversely impact the RCSI, its students, its staff and its business partners. Some examples of confidential information include:
    - Student/ staff personal data (Except that which is restricted);
    - Patient /client medical records (Except that which is restricted);
    - Unpublished medical Research;
    - Staff personal records;
    - Financial data / budgetary Reports;
    - Service plans / service performance monitoring reports;
    - Draft reports;
    - Audit reports;
    - Purchasing information;
    - Vendor contracts / Commercially sensitive data;
    - Data covered by Non-Disclosure Agreements;
    - Passwords / cryptographic private keys;
    - Data collected as part of criminal/HR investigations;
    - Incident Reports.

- **RCSI Network:** The data communication system that interconnects different RCSI Local Area Networks (LAN) and Wide Area Networks (WAN).
- **Information:** Any data in an electronic format that is capable of being processed or has already been processed.
- **Information Owner:** The individual responsible for the management of a RCSI Department/School/Faculty.
- **Information Technology (I.T.) resources:** Includes all computer facilities and devices, networks and data communications infrastructure, telecommunications systems and equipment, internet/intranet and email facilities, software, information systems and applications, account usernames and passwords, and information and data that are owned or leased by the RCSI.
- **Information System:** A computerised system or software application used to access, record, store, gather and process information.
- **Line manager:** The individual a user reports directly to.

- **Network Administrators:** These are the individuals responsible for the day to day management of a RCSI network domain. Also includes RCSI personnel who have been authorised to create and manage user accounts and passwords on a RCSI network domain.
- **Network Domain**: A set of connected network resources (Servers, Computers, Printers, Applications) that can be accessed and administered as group with a common set of rules
- **Personal Information:** Information relating to a living individual (i.e. RCSI employee, student) who is or can be identified either from the Information or from the information in conjunction with other information. For example: - an individual's name, address, email address, photograph, date of birth, fingerprint, racial or ethnic origin, physical or mental health, sexual life, religious or philosophical beliefs, trade union membership, political views, criminal convictions etc.
- **Privacy:** The right of individual or group to exclude themselves or information about themselves from being made public.
- **Process / Processed / Processing:** Performing any manual or automated operation or set of operations on information including:
    - Obtaining, recording or keeping the information;
    - Collecting, organising, storing, altering or adapting the information;
    - Retrieving, consulting or using the information;
    - Disclosing the information or data by transmitting, disseminating or otherwise making it available;
    - Aligning, combining, blocking, erasing or destroying the information.
- **Remote Access:** Any connection to the RCSI network(s) or information systems that originates from a computer or device located outside of the RCSI network.
- **Restricted Information:** Highly sensitive confidential information. The unauthorised or accidental disclosure of this information would seriously and adversely impact the RCSI, its students, its staff and its business partners. Some examples of restricted information include:
    - Unpublished financial reports
    - Strategic corporate plans
    - Sensitive medical Research
- **System Administrator:** The individual(s) charged by the designated system owner with the day to day management of RCSI information systems. Also includes the RCSI personnel and third parties who have been authorised to create and manage user accounts and passwords on these applications and systems.
- **Third Party Commercial Service Provider:** Any individual or commercial company that have been contracted by the RCSI to provide goods and/or services (for example, project / contract management, consultancy, information system development and/or support, supply and/or support of computer software / hardware, equipment maintenance, data management services, patient / client care and management services etc.) to the RCSI.
- **Users:** Any authorised individual using any of the RCSI's I.T. resources.

Appendix B: Supporting Policies:

- Acceptable Usage Policy
- Remote Access Policy
- Data Protection Policies