ICT Security Policy

Policy Number:
015-2014

Academic Year:
2024/2025 Onwards

Target Audience:
All staff, students and third parties

Summary of Contents
This Policy provides a framework for security of all Information and Communication Technologies (ICT) in use throughout SERC.

Enquiries
Any enquiries about the contents of this document should be addressed to:

Title: Chief Technology Officer

E-mail: policies@serc.ac.uk

Review Information:

First Created: May 2009

Last Reviewed: October 2024

Next Review: June 2025

Change Type at last Review:

~~No~~/Minor~~/Significant~~ (delete as appropriate)

Approval/Noting By:

CMT: November 2024

Lead GB Committee: Finance & Staffing

Governing Body Approval: November 2024

Related Documents:
ICT Systems and Services SOP

Superseded Documents (if applicable):
42-2008

Date of Equality of Opportunity and Good Relations Screening (Section 75):
July 2016

Date of Last Accessibility Screening:
June 2024

Contents

1.0 Change History

Changes to this SOP are documented in Appendix 1 of this document. When reading electronic copies of this document, you can click here to view the change history.

2.0 Abbreviations

The definition of abbreviations used within this policy are as follows:

CMT (College Management Team)
The senior management team within the college.

CTO
Chief Technology Officer

ICSC (Information & Cyber Security Committee)
The committee responsible for monitoring cyber & information security within the college.

Cyber Essentials
Cyber Essentials is a UK government-backed, industry-supported scheme to help organisations protect themselves against common online threats.

NIST CSF
The NIST Cybersecurity Framework (CSF) is a set of voluntary guidelines designed to help organizations assess and improve their ability to prevent, detect, and respond to cybersecurity risks. Developed by the U.S. National Institute of Standards and Technology (NIST).

Microsoft Secure Score
Microsoft Secure Score is a set of technical recommendations that allows Microsoft Customers to monitor the state of their security posture across identity, devices, information, apps, and infrastructure. It also enables benchmarking an organization's status over time and comparisons with other organizations.

ITS (IT & Services)
The college department responsible for the delivery of computing services at SERC.

3.0 ICT Security Policy Statement

The College is committed to ensuring that information security is given the highest possible degree of importance. Information is central to our core function, and it is our aim to ensure that the confidentiality, integrity and availability of this information is protected at all times.

The aim of the ICT security policy is to preserve:

1. Confidentiality: data access is confined to those with specified authority to view the data
2. Integrity: all system assets are operating correctly according to specification and in the manner that the current user believes them to be operating
3. Availability: information is delivered to the right person as and when needed

The Information Security Management System is established in-line with NCSC Cyber Essentials, NIST Cybersecurity Framework and Microsoft Secure Score. These frameworks are used to identify, assess and control the risks associated with information security. Our overall objective is to continually improve the information security controls within the organisation.

The College will ensure that we continually identify and assess the threats to information security with which we are faced and will develop controls and systems that are aimed at controlling such threats and minimising the risk of information security breaches.

In support of this policy, the College has developed specific policies and procedures aimed at the management of information security. All staff have specific responsibility for ensuring that the requirements of these policies are adhered to, and all staff will receive training in relation to these policies and procedures.

The Chief Technology Officer (CTO), via the ICSC is responsible for implementation of the ICT security policy and procedures. However, all users have responsibilities for the security and safety of College ICT systems and the information held on these systems. All users are to be made aware of the policies and procedures set out in this document. Each user is responsible for maintaining system security to the extent laid down in this document.

This policy, with approval from the ICSC, may be altered when required to reflect changes to the configuration of its systems and applications and to ensure continued compliance with statutory and other legal requirements. Users will be notified of any material changes to this policy.

If you have any questions about this policy, please contact the CTO in the first instance.

4.0 Introduction and Scope

The purpose of this policy is to protect College, including partner and other 3rd party information assets from all threats, whether internal, external, deliberate, or accidental.

This document provides a hight level framework for security of all Information and Communication Technologies (ICT) in use throughout the College. All other policies and procedures operate under the context of this policy, including where individual systems may already have developed a security policy specific to its individual system policies.

The data stored and processed within college computer systems, both stand-alone and networked, represents one of the Colleges most valuable assets. It is essential that all ICT systems within the organisation are protected to an adequate level from all likely events which may jeopardise core activities.

Within College information systems, users handle information which may be personally or commercially sensitive and, on many occasions, will fall under 'Special Category' status as defined in the Data Protection Act. All staff who develop, operate, maintain, or use ICT systems have an explicit obligation to preserve the security of those systems.

The policy statement and associated procedures aim to provide direction in relation to safeguarding the integrity and confidentiality of information held on College computing systems.

4.1 Objectives

College policies & operating procedures should ensure that:

1. ICT used in the College is properly assessed for risks and threats to security.
2. Appropriate levels of security are applied to maintain the confidentiality, integrity and availability of Information and ICT.
3. All staff are aware of their roles, responsibilities, and accountability for information security.
4. A means is established to communicate awareness of information security issues, their impact on the College for management, staff and students.
5. Procedures to identify, protect, detect, respond, investigate, resolve & recover from security breaches are in place and are dealt with consistently throughout the College.
6. Relevant legislation and regulatory requirements are complied with.
7. Plans are in place to ensure business continuity for all business-critical systems.
8. Monitoring arrangements exist to audit the ongoing effectiveness of the information security arrangements in the College.

4.2 Scope

This policy and associated ICT system procedures apply to all College information and data, as well as computer systems/equipment including mobile and remote access and computer networks, regardless of location i.e. both on and off College premises.

This policy and associated procedures apply to:

1. Employees and students of SERC accessing or using ICT systems.
2. Contractors, while working on College premises or accessing or using ICT systems.
3. Third Parties/Partners associated with the College accessing or using ICT systems.

4. Temporary and Agency Staff accessing or using ICT systems.

4.3 Related Policies & SOPs

There are a range of additional polices & procedures in place to support the security & operation of College systems. These are:

- Acceptable ICT Use Policy
- E Safety Policy
- Data Protection Policy (Sector Policy)
- Information Governance Policy
- Records Management Policy
- ITS Student Device Loan
- ITS Disaster Recovery Policy
- Information Systems (Electronic) Incident Management Policy
- Access to Information (FOI and EIR) Policy
- Application Management SOP
- Backup & Restore SOP
- Device Lifecycle SOP
- ITS Disaster Recovery SOP
- ICT Systems and Services SOP
- User Account Management SOP

5.0 Governance

The CTO, through the ICSC, is responsible for the security and integrity of data held on College systems by specifying, installing and maintaining adequate ICT equipment and security systems. However, all users have responsibility for the security and safety of College ICT systems and the information held on those systems.

5.1 Legislation

Some of the issues of ICT security are governed by legislation, and steps must be taken to ensure College compliance with relevant requirements.

Currently the legislation includes but is not limited to:

1. Data Protection Act (2018): - Appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of, personal data and against loss of personal date.
2. Computer Misuse Act (1990): - This Act cites unauthorised access to any computerised system and the introduction of malicious software as criminal offences.
3. The Obscene Publications Act (1958 & 1964) – Defines the law for preventing the publication for gain of obscene matter and the publication of things intended for the production of obscene matter.
4. Freedom of Information Act (2000) - Defines the right of access to information held by Public Authorities.
5. Health & Safety at Work (NI) Order (1978) - Defines the need to secure the health, safety & welfare of persons at work.

6. Regulatory Investigative Powers Act (2000) – Defines the need to monitor staff actions in terms of illegal abuse.
7. Terrorism Act 2006 – Extends Intelligence services warrants to enable the interception communications.
8. Counter Terrorism and Security Act 2015 – Relates the need to secure IT systems, protect sensitive data and monitor/log potentially dangerous activity.

5.2 Monitoring

This policy is designed to reduce the risk to the College and its reputation if ICT Systems were to be used inappropriately. Users should be aware that their use of College ICT systems, including Internet and E-Mail will be monitored and electronically logged.

Monitoring will be conducted in accordance with relevant UK and EU Law including:

1. Regulation of Investigatory Powers Act 2000
2. Lawful Business Practice Regulations 2000
3. Data Protection Act 2018
4. Part 3: Monitoring at Work, as issued by the UK Information Commissioner

5.3 Non-Compliance

All breaches of the ICT Security Policy will be addressed. Failure to comply with this policy by users is a serious matter and may result in the initiation of disciplinary action. Initial Investigations into actual or suspected breaches of this policy will be conducted by the CTO.

Repeated or serious breaches will be passed on to appropriate Senior Manager and the ICSC for further investigation and action. It is the responsibility of all staff and students to report actual or suspected non-compliance.

6.0 Incidents

Incidents, such as a disaster or data breach, will be dealt with under the appropriate SOP/Policy dependant on the nature of the incident.

7.0 Communication

This Policy will be available for all users via College intranets and public Website. It will be made available, on request, in alternative formats including large print, braille, audio, and in minority languages to meet the requirements of those who are not fluent in English.

8.0 Policy Review

This policy will normally be reviewed annually, however if changes are required outside of this cycle to reflect changes in circumstance, this policy will passed through the relevant approval processes at the earliest opportunity.

Appendix 1: Document Change History

Version	Date	Change Detail
1.0	May 2009	Initial Version
1.1	June 2020	Amendments Made to: Section 3 - Grammar Correction. Section 4 - Altered sentence to be more concise. Section 8 - Updated review cycle text.
1.2	June 2021	Reviewed in June 2021 – no amendments required
1.3	01/06/2022	Changes to layout only: 1. Converted bulleted lists to numbered lists for easier referencing. 2. Moved change history to end of document. 3. Review date changed to every two years.
2.0	03/06/2024	Transferred to new accessibility template. No other changes required.
2.1	29/10/2024	Amendment made to: Section 3, Paragraph 3 – Added reference to NCSC Cyber Essentials and Microsoft Secure Score New Section: Section 4.3 – A list of relation policies & SOPs
2.2	November 2024	Cover sheet updated and review changed to annually