INSPIRING. TRANSFORMING. ENRICHING.

POLICY TITLE

ICT SECURITY POLICY

Academic Year: 2016/17 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:	Head of ICT Infrastructure
Address:	Bangor Campus Castle Park Road Bangor BT20 4TD
Tele:	028 9127 6600 X 8205
Mob:	07899958209
E-mail:	aemmett@serc.ac.uk

Final Approval by:

CMT – 06/05/2009

Governing Body – May 2009

Policy Number: 015-2014

First Created:	May 2009
Last Reviewed:	May 2017 June 2018
Next Review Due:	May 2019

Related Documents:

ICT Systems Procedures (SOPs)

Superseded Documents (if applicable):

42-2008

Equality of Opportunity and Good Relations Screening Information (Section 75):

Date Policy Screened – July 2016

1. ICT Security Policy Statement

The Board of Governors, through the Security Management Group 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:-

- Confidentiality: data access is confined to those with specified authority to view the data;

- Integrity: all system assets are operating correctly according to specification and in the manner that the current user believes them to be operating;

- Availability: information is delivered to the right person as and when needed;

The Information Security Management System is established in-line with best practice, namely, ISO27001:2013 and this system is 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.

We 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 we have 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 Head of ICT Infrastructure, via the Security Management Group is responsible for implementation of the ICT security policy and procedures. However all SERC users have responsibilities for the security and safety of SERC ICT systems and the information held on the 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 ICT Security Management Group, 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 ICT policy.

If you have any questions about this policy, please contact the Head of ICT Infrastructure in the first instance.

2. Purpose

The purpose of this policy is to protect South Eastern Regional College (SERC) information assets from all threats whether internal, external, deliberate or accidental.

This document provides a framework for security of all Information and Communication Technologies (ICT) in use throughout SERC. 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 our computer systems, stand-alone and networked, represents one of the SERC most valuable assets. It is essential that all ICT within SERC environment are protected to an adequate level from all likely events which may jeopardise our core activities.

Within SERC information systems, users handle information which may be potentially sensitive and on many occasions restricted and confidential under legislation such as the Data Protection Act. All SERC staff who develop, operate, maintain or use ICT 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 the SERC computers.

2.1 Objectives

The guidance in this document aims to ensure that:

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

3. Scope

The policy and associated ICT system procedures apply to all SERC Information/Data both on and off our premises, computer systems/equipment including mobile and remote access and computer networks.

The policy and procedures include, but are not limited to:

- Employees and students of SERC accessing or using ICT
- Contractors, while working on SERC premises or using/accessing SERC ICT
- All Third Party Associations with SERC.
- Temporary and Agency Staff

4. Governance

The Head of ICT Infrastructure, through the Security Management Group (SMG), is responsible for the security and integrity of data held on SERC systems by specifying, installing and maintaining adequate ICT equipment and security systems. However, all SERC users have responsibility for the security and safety of SERC ICT systems and the information held on those systems.

4.1 Legislation

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

Currently the legislation includes but is not limited to: -

- Data Protection Act (1998): - Appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of, personal data and against loss of personal date.
- Computer Misuse Act (1990): - This Act cites unauthorised access to any computerised system and the introduction of malicious software as criminal offences.
- 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.
- Freedom of Information Act (2000) - Defines the right of access to information held by Public Authorities.
- Health & Safety at Work (NI) Order (1978) - Defines the need to secure the health, safety & welfare of persons at work.
- Regulatory Investigative Powers Act (2000) – Defines the need to monitor staff actions in terms of illegal abuse.
- Environment Act & Hazardous Waste Regulations
- WEEE Directive and the Battery Directive defines the purpose for which organisations can lawfully dispose of ICT Equipment.

4.2 Monitoring of this ICT Security Policy

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

Monitoring is performed in accordance with relevant UK and European Law, such as, The Lawful Business
Practice Regulations 2000, European Parliament Directive 95/46/EC, Directive 97/66/EC, Directive 2002/58/EC, Employment Practices Data Protection Code, Part 3: Monitoring at Work, as issued by the UK Information Commissioner

In order to regulate this policy, there will be regular and consistent monitoring to ensure adherence. This will be addressed in its entirety, as any breaches of this policy will be recorded regardless of the section they are contained in.

The Lawful Business Practice Regulations 2000, European Parliament Directive 95/46/EC, Directive 97/66/EC, Directive 2002/58/EC and other relevant EC/UK/ROI policies and guidance require staff and students to inform the SMG if there is a possibility that interceptions of communications might take place.

4.3 Non Compliance

All breaches of the ICT Security Policy will be addressed. Failure to comply with this policy by SERC 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 Head of ICT Infrastructure

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

5. Communication Plan

This Policy will be uploaded to the College Intranet for staff reference.