INSPIRING. TRANSFORMING. ENRICHING.

POLICY TITLE

ACCEPTABLE ICT USE POLICY

Academic Year: 2021/22 onwards

Target Audience:

All Staff/All Students/3rd Parties

Summary of Contents:

General principles of using computing services at any SERC campus

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

Title: Chief Technology Officer
Address: Bangor Campus
Castle Park Road
Bangor
BT20 4TD

Tele: 028 9127 6600 X 8205
Mobile: 07899958209
E-mail: aemmett@serc.ac.uk

Approval by:

CMT – 8 June 2020

Audit Committee – 17 June 2020

Governing Body – 29 June 2020

Policy Number: 001-2014

First Created: January 2008
Last Reviewed: May 2017
June 2018
May 2019
June 2020
June 2022
Next Review Due: June 2024

Related Documents:

Superseded Documents (if applicable):

05-2008

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

Date Policy Screened - June 2016

Contents

1.0 CHANGE HISTORY 1

2.0 ABBREVIATIONS 1

3.0 INTRODUCTION AND SCOPE 2

4.0 ACCEPTABLE USE 2

5.0 UNACCEPTABLE USE 2

6.0 OTHER USE 3

7.0 PERSONAL SAFETY 3

8.0 MONITORING 3

9.0 COMPLIANCE WITH POLICY 4

10.0 COMMUNICATION 4

11.0 POLICY REVIEW 4

APPENDIX 1: DOCUMENT CHANGE HISTORY 5

APPENDIX 2: DECLARATION OF COMPLIANCE 6

1.0 Change History

Changes to this SOP are documented in Appendix 1 of this document. When reading electronic copies of this document, you may 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.

Computing Services
"Computing Services" can be defined as the use of any item of SERC, or personally owned computing equipment, (i.e. PCs, macs, laptops, Macbooks, tablets, mobile phones, servers) for running of applications and for accessing networked services such as file, print, e-mail and internet.

JANET
"JANET" (Joint Academic NETwork) is the trademark used for the collection of networking services and facilities which support communication requirements of the UK education and research community.

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

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

Network Proxy
A specialist service that can be used to allow web browsing traffic to appear to originate from another site, bypassing security monitoring systems.

Tor Network
The Tor network makes it more difficult to trace a user's Internet activity by concealing a user's location and usage from security monitoring systems.

3.0 Introduction and Scope

This document defines South Eastern Regional College's (SERC) policy for the acceptable use of its computing and data communications facilities. Users are bound by this policy at all times when using equipment, software or services provided by the College.

4.0 Acceptable Use

Acceptable use of SERC's information systems & facilities is defined as their use for the College's teaching, learning, research and administrative activities. For students, this includes research and assignment work. For staff, this includes administrative, teaching and research activities.

Users must act in accordance with UK law, and material imported or transmitted across international boundaries must not contravene international laws or treaties.

5.0 Unacceptable Use

Unacceptable use is:

1. Creation or transmission, or causing the transmission, of any offensive, obscene or indecent images, data or other material.
2. Creation or transmission of material with the intent to cause annoyance, inconvenience or needless anxiety.
3. Creation or transmission of material with the intent to defraud or assist criminal activity, e.g. Phishing
4. Creation or transmission of defamatory material.
5. Creation or transmission of material such that this infringes the copyright of another person.
6. Creation or transmission of unsolicited bulk or marketing materials to other users.
    a. In the case of emails to college provided email address, consent should be obtained from a member of college management.
    b. In the case of emails to any private email address, consent should be obtained from the account owner and any opt-out preferences **must** be respected.
7. The revelation, publication, theft or destruction of information/data which is considered personal or confidential. This includes passwords, user account information and any SERC business or the personal details of one or more individuals.
8. Creation or transmission of covert audio or video recordings without the explicit consent of individual participants. Consent **must** be sought.
9. The use of the College's information systems to cheat, plagiarise or steal the work of others.
10. Deliberate unauthorised access to networked facilities or services, including interception of network traffic.
11. Deliberate avoidance or bypassing of network monitoring and security measures (e.g. proxy sites, Tor network Browser etc)
12. Attempts to block or wilfully ignoring important processes such at the scheduled updating of college equipment or software.
13. Refusal to follow instruction from ITS College's IT & Services Department when trying to resolve security matters.

14. Misuse, inadequate use, and damage, either deliberate or through negligence, of college loaned equipment.
15. Operating a business over the College's information systems facilities without permission.
16. Where the JANET Infrastructure is being used to access another network, any violation of access policies of that network will be regarded as unacceptable use of JANET
17. Deliberate activities having, with reasonable likelihood, any of the following characteristics:
    a. wasting staff effort or networked resources
    b. corrupting or destroying other users' data
    c. violating the privacy of other users
    d. disrupting the work of other users
    e. denying service to other users (for example, by deliberate overloading of systems)
    f. continuing activities that the college has requested to cease because it is causing disruption to services
    g. the introduction of "viruses" or other harmful software. Any other use deemed unacceptable by supervisory staff.

6.0 Other Use

Occasional and moderate use of college information systems facilities for private use is permitted, provided it does not occupy class time or the employer's time, and does not entail trading or selling. Your college e-mail address must not be provided in relation to the private use of any on-line service.

7.0 Personal Safety

The college has provided all users with an online 'e-Safety' module. This module is provided to help users understand what is safe and acceptable activity when using computing facilities. The module can be found on staff & student intranets.

8.0 Monitoring

All users of ICT services have a reasonable expectation of privacy. However, SERC also has responsibilities to ensure that its computing facilities are safe, secure and used for legitimate purposes. The College's IT & Services Department, in the course of normal business, collects a wide range of diagnostic & audit data based on device and network usage. This data is used for the following purposes:

1. to establish facts to ascertain compliance with regulatory practices
2. in the interests of security
3. to prevent or detect misuse
4. to investigate or detect unauthorised use of networked systems
5. to secure effective system operation
6. in association with specialist training

Should SERC suspect that the AUP is being violated, the suspected user(s) will forfeit any right to privacy so that SERC can enforce its requirement to protect the integrity of computing resources, data and the rights of other users. SERC therefore reserves the right to examine material stored on, or transmitted through its facilities, if there is a reasonable cause to believe that the standards for acceptable use are being violated by a user.

For the avoidance of doubt, interception of communications, access to logs or the examination of file/email storage will only be made by persons authorised, typically IT support staff acting in relation to their primary area of responsibility.

9.0 Compliance with Policy

It is the user's responsibility to ensure compliance with this policy. A paper-based declaration of compliance has also been provided in Appendix 2 for areas which require it. However, on-going use of computing facilities by users constitutes acceptance of this Acceptable Use Policy.

Users may be held personally liable for the consequences of misuse. Violation may result in disciplinary action. Where violation is illegal or unlawful, or results in loss or damage to College resources or the resources of third parties, the matter may be referred for legal action.

Where necessary, on violation of the policy, services may be withdrawn from a user. This may take one of two forms:

1. Suspension of service. Such a suspension would be made on the judgement of the Information & Cyber Security Committee or a Head of Department in conjunction with a Senior member of the IT & Services Department. Service would be restored when the matter has been resolved.
2. Indefinite withdrawal of service. This would arise should a violation persist after appropriate warning has been given, and only on the instruction of a disciplinary authority. Restoration will be made only when the disciplinary authority is satisfied that appropriate steps have been taken to ensure acceptable behaviour in future.

10.0 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.

11.0 Policy Review

This policy will normally be reviewed every 2 years, 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

Date of Change	Approved By	Change Detail
January 2009	AE	Initial document creation
June 2020	AE	Amendments made to: 1. Page 3 – New Section on personal safety. 2. Page 4 – New Line referring to form in Appendix 3. Page 5 – Updated review cycle text
01/06/2022	AE	Amendments made: 1. Converted bulleted lists to numbered lists for easier referencing 2. Moved change history to end of document. 3. Added section 5.0 points 12 – 14 reflecting additional unacceptable behaviours.

Appendix 2: Declaration of Compliance

Content on next page

Declaration of Compliance

I have read and understood the conditions outlined in this policy and do hereby agree to comply with the acceptable use of computing services and facilities within SERC. I will not attempt to use such computing services for any unacceptable use as outlined in this policy document.

Name (Capitals) _____

Signature _____ **Date** _____