Acceptable ICT Use Policy

Policy Number:
001-2014

Academic Year:
2025/2026

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

E-mail: policies@serc.ac.uk

Review Information (Responsible Owner):
First Created: January 2008

Last Reviewed: March 2026

Next Review: March 2027

Change Type at last Review:
~~No/Minor/~~Significant (delete as appropriate)

Approval/Noting By:
CMT: 27 April 2026

Lead GB Committee: Finance & GP

Governing Body Approval: April 2026

Related Documents:
N/A

Superseded Documents (if applicable):
05-2008

Date of Equality of Opportunity and Good Relations Screening (Section 75):
Policy Screened - June 2016

Date of Last Accessibility Screening:
May 2025

Contents

1.0 CHANGE HISTORY 1
2.0 ABBREVIATIONS 2
3.0 INTRODUCTION AND SCOPE 3
4.0 ACCEPTABLE USE 3
5.0 UNACCEPTABLE USE 3
6.0 OTHER USE 4
7.0 PERSONAL SAFETY 4
8.0 USE OF PERSONAL DEVICES 5
9.0 MONITORING 5
10.0 COMPLIANCE WITH POLICY 5
11.0 REPORTING & HANDLING NON-COMPLIANCE 6
12.0 COMMUNICATION 6
13.0 POLICY REVIEW 6
APPENDIX 1: DOCUMENT CHANGE HISTORY 7
APPENDIX 2: DECLARATION OF COMPLIANCE 8

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.

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.

DTAC (Digital Trust & Assurance Committee)
The committee responsible for monitoring cyber, information security & AI risk 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. In summary, the college expects all users to the following key:

1. Use College ICT for legitimate purposes
2. Protect data and privacy
3. Not attempt to bypass security
4. Follow instructions from IT & Services

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.

The use of artificial intelligence tools and services must align with College guidance.

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. Uploading College data which is considered personal or confidential to external systems or cloud services not approved by the College.
9. Creation or transmission of covert audio or video recordings without the explicit consent of individual participants. Consent must be sought.

10. The use of the College's information systems to cheat, plagiarise or steal the work of others This includes the use of Artificial Intelligence (AI) tools.
11. Deliberate unauthorised access to networked facilities or services, including interception of network traffic.
12. Deliberate avoidance or bypassing of network monitoring and security measures (e.g. proxy sites, Tor network Browser etc)
13. Attempts to block or wilfully ignoring important processes such at the scheduled updating of college equipment or software.
14. Refusal to follow instruction from the College's IT & Services Department when trying to resolve security matters.
15. Misuse, inadequate use, and damage, either deliberate or through negligence, of college loaned equipment.
16. Operating a business over the College's information systems facilities without permission.
17. 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
18. 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 'Digital 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.

Students who may be suffering from online/digital bullying or harassment should speak to a member of staff.

Any member of staff who is concerned about the wellbeing of a student is expected to raise their concern through the College's Cause for Concern App.

Staff who experience concerns relating to technology that affect themselves can approach the College network team who will advise on the best way to address any issues/concerns.

8.0 Use of Personal Devices

The college supports & encourages the use of personally owned devices (BYOD). This policy extends to those devices when connected to College operated networks such as eduroam and is always applicable when carrying our activity using college issued user accounts. More information is available in the ICT Systems and Services SOP.

9.0 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. Monitoring activities are undertaken in accordance with applicable legislation and are proportionate, targeted, and subject to appropriate authorisation. 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.

10.0 Compliance with Policy

Use of ICT systems must comply with applicable data protection legislation, including UK GDPR, the Data Protection Act 2018, and related College policies.

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.

10.1 Reporting & Handling Non-Compliance

In the event of suspected non-compliance with this policy, staff and students should promptly report their concerns to their immediate line manager or lecturer. Alternatively, reports may be directed to the College's IT & Services Department, either via email, telephone, or through the official service desk portal. Where appropriate, concerns may be escalated to the Digital Trust & Assurance Committee for further investigation and action.

If the matter involves sensitive information or requires anonymity, individuals may make use of confidential reporting channels provided by the College, such as the whistleblowing policy. All reports will be handled in accordance with College confidentiality guidelines and relevant data protection legislation.

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 a Head of School/Department in conjunction with a Senior member of the IT & Services Department, normally the CTO. 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.

In exceptional cases, where a member of the college network team considers that the actions or activity of any user poses an immediate risk to college systems or data, the network team is authorised to temporarily suspend access until a more compete threat assessment can be made.

11.0 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.

12.0 Policy Review

This policy will 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	January 2009	Initial document creation
1.1	June 2020	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
1.3	May 2024	Reviewed for Accessibility and moved to new template
1.4	June 2024	No Changes required.
1.5	November 2024	Cover page updated and review changed to annually
1.6	May 2025	Added text to instruct for referral to cause for concern app to section 7.
1.7	March 2026	Section 3 – Key Principals have been added Section 4 – Added reference to AI use Section 8 – Fixed Spelling mistake Section 5 Point 8 – Added reference to unapproved cloud storage Section 5 Point 10 – Added reference to AI tools Section 9 – Added a wording to be clearer about lawful basis and proportionality Section 10 – Added reference to UK GDPR Section 10 – Moved Reporting & Handling Non-Compliance into a new section (11) and elaborated on ownership, process & responsibilities

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 _____