INSPIRING. TRANSFORMING. ENRICHING.

POLICY TITLE

E-SAFETY POLICY

Academic Year: 2021/22 onwards

Target Audience:

Those with authorised access to College ICT systems, including Staff, Students/Trainees and Governing Body members.

Summary of Contents:

The e-Safety Policy sets out the College's implementation of appropriate safeguards to protect authorised users of the internet and other forms of electronic communication and to satisfy SERC's wider duty of care.

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: 034-2014

First Created: 31 March 2014
Last Reviewed: May 2016
May 2017
May 2018
May 2019
June 2020
June 2022
Next Review Due: June 2024

Related Documents:

Acceptable Use Policy

ICT Services SOP

Superseded Documents (if applicable):

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

Date Procedure Screened – July 2016

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 may click here to view the change history.

2.0 Abbreviations

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

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.

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

3.0 Introduction and Scope

South Eastern Regional College (SERC) recognises the benefits and opportunities which new technologies offer to teaching and learning. SERC provides internet access to all students and staff and encourages the use of technologies in order to enhance skills, promote achievement and enable lifelong learning. However, the availability, accessibility and global nature of the internet and different technologies means that there are associated potential risks and challenges.

The overall approach is to implement appropriate safeguards within the College, while supporting staff and students to identify and manage risks independently and with confidence. This is achieved through a combination of security measures, training, guidance and implementation of SERC Policies and Standard Operating Procedures (SOPs). The intention is to, in so far as is practically possible, make students and staff stay 'e-Safe' and to satisfy the College's wider duty of care.

This Policy applies to those with authorised access to the College ICT systems both on College premises and remotely. This includes students, staff and members of the Governing Body. Any authorised user of College IT systems must adhere to terms & conditions outlined in the College Acceptable Use Policy. The e-Safety Policy applies to all use of the internet and forms of electronic communication such as email, social media sites etc.

This e-Safety policy should be read alongside other relevant college documents e.g. Acceptable Use Policy and ICT Systems & Services SOP.

4.0 Roles and Responsibilities

4.1 General

There are clear lines of responsibility for e-Safety within the College:

1. All staff are responsible for ensuring the safety of students and should report any concerns immediately to their line manager. If deemed necessary, a member of staff may also raise a 'Cause for Concern' via the staff Intranet.
2. Students should primarily report any concerns to their Course Co-ordinator, but in their absence or in case of an emergency, may report concerns to any member of SERC staff.
3. The Chief Technology Officer, in conjunction with the relevant departmental manager is responsible for investigating e-Safety incidents.
4. Serious incidents may be referred to the Director of Curriculum Services, HR or College Management Team.

4.2 Security

The College will do all that it can to make sure the SERC network is safe and secure. Every effort will be made to keep security software up to date. Appropriate security measures will include the use of web content filtering software and firewalls. College servers and end user devices will be secured to prevent accidental or malicious access of College systems and information. Internet access & Device usage will also be logged to assist potential investigations into e-Safety incidents.

4.3 Protection of Personal Information

The College collects and stores the personal information of students and staff regularly e.g. names, dates of birth, email addresses and assessment materials. The College will keep that information safe and secure and will not pass it onto anyone else without the express permission of the staff member or student.

4.4 Use of Images and Videos

No image/photograph of students, staff members, 3rd party contractors or other members of the public may be copied, downloaded, shared or distributed online without the consent of the person/s within the image. Photographs of activities on College premises should be considered carefully and, if they contain identifiable persons, consent should be obtained from the relevant individuals before being published. Staff members have further obligations which must be adhered to. These are detailed in the Communications & Marketing SOP.

4.5 Acceptable Behaviour

Users of ICT systems may at some point be required use one or more forms of electronic communication such as email, mobile phones, social media sites (if access is permitted), games consoles, video conferencing and web cameras for College business and educational purposes. Whether offline or online, communications by users should be courteous and respectful at all times.

Any reported incident of bullying, harassment, grooming, identity theft or other unacceptable conduct will be treated seriously and in line with the student and staff disciplinary codes. This includes communications using social media platforms such as Facebook, twitter etc, where the activity may impact on the welfare of another student or staff member. Clarity on what is deemed acceptable use is detailed in the college's Acceptable Use Policy.

5.0 End User Education and Training

With the current, unlimited nature of internet access, it is impossible for the College to eliminate all risks for users. The College will support users to enable them to stay 'e-Safe' through regular training and education. This training will be made available on staff and student intranets and will also part of the College induction process. This will provide individuals with skills to be able to identify risks independently and manage them effectively.

6.0 Incidents and Response

Where an e-Safety incident is reported to the College, the College will act immediately to prevent, it necessary & as far as reasonably possible, any harm or further harm occurring.

Following any incident, the Chief Technology Officer, in conjunction with the relevant departmental manager, will investigate what has happened and decide on the most appropriate and proportionate course of action. Serious incidents may be referred to the Director of Curriculum Services, HR or College Management Team.

The outcome of the investigation may result in sanctions being put in place, the involvement of the appropriate external agencies, or the matter may be resolved internally depending on the seriousness 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 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
March 2014	AE	Initial document creation
June 2020	AE	Amendments made to: 1. Section 3 – New word added 2. Section 3 – Fixed grammar 3. Section 4.4 – New Sentence 4. Section 8 – 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.