SERC

INSPIRING. TRANSFORMING. ENRICHING.

POLICY TITLE

E-SAFETY POLICY

Academic Year: 2016/17 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: Head of ICT Infrastructure
Address: Bangor Campus
Castle Park Road
Bangor
BT20 4TD

Tele: 028 9127 6600 X 2767
Mobile: 07919 597724
E-mail: jcunningham@serc.ac.uk

Final Approval by:

CMT – 27 May 2014

Governing Body – 24 June 2014

Policy Number: 034-2014

Created: 31 March 2014
Last Reviewed: May 2016
May 2017
Review Due: May 2018

Related Documents:
Acceptable Use Policy
ICT Services SOP

Superseded Documents (if applicable):

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

Date Policy Screened: July 2016

1.0 Purpose

1.1 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 approach is to implement appropriate safeguards within the College, while supporting staff and students to identify and manage risks independently and with confidence. This can be achieved through a combination of security measures, training, guidance and implementation of SERC Policies and Standard Operating Procedures (SOPs). The intention is to do all possible to make students and staff stay e-safe and to satisfy SERC's wider duty of care. This e-safety policy should be read alongside other relevant college documents e.g. Acceptable Use Policy and ICT Services SOP.

2.0 Scope

2.1 This Policy applies to those with authorised access to the College ICT systems both on SERC premises and remotely. This includes students, staff and members of the Governing Body. Any authorised user of College IT systems must adhere to and sign a hard copy of the 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.

3.0 Process

3.1 Roles and Responsiblities

There are clear lines of responsibility for e-safety within the College. All staff are responsible for ensuring the safety of students and should report any concerns immediately to their line manager. When informed about an e-safety incident, staff members must take particular care not to guarantee any measure of confidentiality towards either the individual reporting it, or to those involved.

3.2 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 filtering software and firewalls. College servers, desktops, laptops, tablets and macBooks will be secured to prevent accidental or malicious access of College systems and information.

3.3 Behaviour

The College will not tolerate any abuse of ICT systems. Whether offline or online, communications by users should be courteous and respectful at all times. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the student and staff disciplinary codes.

3.4 Communications

The College requires all users of ICT systems to use all forms of 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.

3.5 Use of Images and Videos

No image/photograph can be copied, downloaded, shared or distributed online without permission from the owner or publisher. Photographs of activities on the College premises should be considered carefully and have the consent of those involved before being published. Approved photographs should not include names of individuals without consent. In all circumstances, compliance with the College Data Protection Policy and SOP is essential.

3.6 Personal Information

SERC collects and stores the personal information of students and staff regularly e.g. names, dates of birth, email addresses and assessed 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.

3.7 Education and Training

With the current unlimited nature of internet access, it is impossible for SERC to eliminate all risks for users. The College will support users to enable them to stay e-safe through regular training and education. This will provide individuals with skills to be able to identify risks independently and manage them effectively.

3.8 Incidents and Response

Where an e-safety incident is reported to the College, the matter will be dealt with very seriously. The College will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring. If a student wishes to report an incident, they can do so to their tutor or to the College e-Safety Officer. Where a member of staff wishes to report an incident, they must contact their line manager as soon as possible. Following any incident, SERC will review what has happened and decide on the most appropriate and proportionate course of action. Sanctions may be put in place, external agencies may be involved or the matter may be resolved internally depending on the seriousness of the incident. Serious incidents will be dealt with by senior management, in consultation with appropriate external agencies.

4.0 Responsible Owner

4.1 The Head of ICT Infrastructure

5.0 Communication

This Policy will be communicated via staff development training and the intranet and 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.

6.0 Review

The impact of the policy will be monitored regularly with a full review being carried out at least once/twice a year. The policy will also be reconsidered where particular concerns are raised or where an e-safety incident has been recorded.