



IT and Cyber Security Policy

Introduction

This policy exists to ensure that all staff and students follow certain basic rules with regard to internet use and use of IT in general. Its aim is to prevent students or staff coming to harm as a result of others accessing intolerant, extremist or hateful web sites. Also, it is here to protect students and staff from cyber bullying. The Principal is responsible for implementing this policy. Further information regarding the appropriate use of technology may be found in the Employee Handbook.

Use of the internet

CES will provide internet access to teachers and students for the primary purpose of study, legitimate research, email access and general internet access. The availability and variety of information on the Internet means that it can be used to obtain material reasonably considered to be offensive. The use of the Internet to access and/or distribute any kind of offensive material, or material that is not work or study related, leaves an individual (staff and students) liable to disciplinary action which could lead to dismissal.

CES Internet and IT provision may not be used for:

- transmitting, retrieving or storing any communications of a discriminatory or harassing nature
- transmitting, retrieving or storing any communications which are derogatory to any individual or group
- obtaining material that would cause offence on the grounds of race, colour, religion, political beliefs, ethnic origin, sexual orientation, gender, age, disability, nationality, marital status,
- engaging in to form of cyber bullying
- searching for obscene, offensive, sexually explicit or pornographic material
- obtaining any material for the purpose of harassment of another person
- establishing communications which are defamatory or threatening
- obtaining material that is unlawful or that infringes on another person's legal rights (e.g illegal downloads)
- conducting internet searches and looking at websites which can in any way be regarded as extremist, intolerant of other's faiths and beliefs, or that challenge the rule of law and the right to individual liberty

Monitoring Use of Computer Systems

CES has the right to monitor electronic information created and/or communicated by students or staff using CES computer systems and networks, including e-mail messages and usage of the Internet. In the majority of cases Centre of English Studies will not monitor its IT or telecommunications systems without providing prior notice to its employees. However, in the following circumstances, CES may monitor and use information without prior and specific consent:

- To check the quality of the work and compliance with operating procedures.
- To ascertain compliance with regulatory practices or procedures.
- To prevent or detect crime.
- To investigate or detect the unauthorised use of the Company's telecoms and IT systems, other instances of possible gross misconduct or breaches of health and safety rules that may jeopardise other employees.

This information may be stored and printed to be used as documentary evidence where appropriate. However, the information will be used only by those Senior Management involved in, and disclosed to third parties associated with, the investigation. For example, lawyers, regulatory bodies, police, and so on.

Remote Access

Only authorized persons may remotely access the CES IT network.

Social networking sites

- Don't search for illegal and inappropriate sites or material.
- Don't accept a friendship request from a student under the age of 18
- Do use the computers for school/study use or to connect with other students in a positive manner.
- Don't bully anyone through blogs, emails, chatrooms, or any other form of internet use
- Don't download anything illegally.
- Do not give your personal contact details to students under the age of 18 including e-mail, home or mobile telephone numbers.
- Don't use the internet to give opinions that are extremist, intolerant of other's faiths and beliefs, or that challenge the rule of law and the right to individual liberty
- Misuse should be reported to a senior member of staff without delay

Any work-related issue or material that could adversely affect CES, its staff or its students must not be placed on a social networking site at any time and via any medium.

Email

The use of the email system is encouraged as its appropriate use facilitates efficiency. Used correctly it is a facility that is of assistance to employees. Inappropriate use however causes many problems including distractions, time wasting and legal claims. The procedure sets out the company's position on the correct use of the E-mail system.

Authorised Use

- Unauthorised or inappropriate use of the email system may result in disciplinary action which could include summary dismissal.
- The email system is available for communication and matters directly concerned with the legitimate business of CES. Employees using the email system should pay particular attention to the following points:-
 - ❖ all comply with company communication standards;
 - ❖ email messages and copies should only be sent to those for whom they are particularly relevant;
 - ❖ email should not be used as a substitute for face-to-face communication or telephone contact. Flame mails (i.e. emails that are abusive) must not be sent. Hasty messages sent without proper consideration can cause upset, concern or misunderstanding;
 - ❖ if email is confidential the user must ensure that the necessary steps are taken to protect confidentiality.
 - ❖ offers or contracts transmitted by email are as legally binding on CES as those sent on paper.
- CES will not tolerate the use of the email system for unofficial or inappropriate purposes, including:-
 - ❖ any messages that could constitute bullying, harassment or other detriment;
 - ❖ personal use (e.g. social invitations, personal messages, jokes, cartoons, chain letters or other private matters);
 - ❖ on-line gambling;
 - ❖ accessing or transmitting pornography

Rules for Acceptable Internet Use:

Everyone using school IT facilities will

- respect the facilities on offer by using them safely and appropriately.
- not deliberately seek out inappropriate websites.
- report any unpleasant material to a senior member of staff immediately
- not download/install program files.
- be polite and respect others when communicating over the Internet.
- not give out any personal information over the Internet.
- not share my login details for websites with others.

Penalty for Security Violation

CES takes the issue of security seriously. Those people who use the technology and information resources of CES must be aware that they can be disciplined if they violate this policy. Upon violation of this policy, an employee may be subject to discipline up to and including dismissal. The specific discipline imposed will be determined on a case-by-case basis, taking into consideration the nature and severity of the violation of the Cyber Security Policy. Discipline which may be taken against an employee shall be administrated in accordance with the CES disciplinary procedure