

E-Safety Policy

August 2011

UNCONTROLLED WHEN PRINTED

Also available in large print (16pt)
and electronic format.

Ask Student Services for details.

www.perth.uhi.ac.uk

Perth College is a registered Scottish charity, number SC021209.



Version Control History

Version Number	Date of Change	Summary of Revisions Made
1	August 2011	Review due date extended from Jan 13 to June 13. Customer and Student Services Manager changed to Student Services Manager, and Learning and Information Services Manager changed to Information Services and Procurement Director throughout. Version number remains stat. Republished 26 Feb 13.
1.1	July 2016	Footer updated to reflect new template model. Role Title Change: Vice Principal, Academic; International and Corporate Services Director; Head of Student Services; Head of Quality
1.2	December 2018	Change of role to Quality Manager.

E-Safety Policy

1 Purpose

- 1.1 Perth College UHI recognises the benefits and opportunities which new technologies offer to teaching and learning and wishes to encourage the use of technology in order to enhance skills and promote achievement. However, the accessible and global nature of the internet and other available technologies requires that we are also aware of potential risks and challenges associated with such use and that the College takes steps to appropriately address these. The purpose of this policy is to detail the approach that the College will take to implement appropriate arrangements in order to identify and manage risks, safeguard and support staff and students, and to promote the safe use of technology.

2 Scope

- 2.1 The policy applies to all students and staff, members of the Board of Management, and all other users of the College's premises or systems who have access to the Information Communications Technology (ICT) systems, both within College buildings and remotely.

The policy applies to all use of the internet and electronic communication tools such as, but not confined to, email, mobile phones, games consoles and social networking sites.

3 Definitions

- 3.1 **E-Safety** encompasses all Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate users about the benefits and risks of using technology and provides safeguards and awareness to enable them to control their online experience.
- 3.2 **ICT (Information Communications Technology)** consists of all technical means used to handle digital information and aid communication, including computer and network hardware, software and data and information management. In other words, ICT consists of IT as well as telephony, broadcast media, and all types of audio and video processing and transmission.
- 3.3 **Social Networking** sites are web-based services that allow individuals to: construct a public or semi-public profile within a bounded system; articulate a list of other users with whom they share a connection; and view and traverse their list of connections and those made by others within the system.
- 3.4 **Personal Data** is data which relate to a living individual, and which could allow the individual to be identified from the data.

Title: E-Safety Policy
Version/Status: 1.2, Final
Approved By/Date: CMT, 08/2011

Effective Publication Date: August 2011

Owner: Depute Principal, Academic
Lead Author: Head of Student Experience
Student Services Manager
Review Timing/Date: 5 Years/2016/17

4 Key Principles

4.1 ICT Security

The College takes steps to ensure that its networks are safe and secure in order to protect both users and the institution. Security software is kept up to date and a range of security measures are in place within the College to prevent accidental or malicious access of systems and information. These measures include firewalls, anti-virus software and password management.

Digital communications, including email and internet postings, over the College network, are monitored in line with the ICT Security and Acceptable Use Policies.

4.2 Risk Assessment

In order for the College to appropriately promote and make available a range of technologies and online platforms, it is necessary for potential risk levels to be considered while such technologies are being planned. The assessment of risk allows both level and nature of risk to both users of the ICT systems and the College to be determined and for corresponding risk management measures to be implemented. Risk is assessed and considered before any new or emerging technology is made available to staff or students on the College's systems.

4.3 Acceptable Use

The College requires all users of its ICT systems and networks to adhere to the standard of behaviour as set out in the Acceptable Use Policy and for staff to work within the Code of Conduct detailed within the Safeguarding Policy.

Unacceptable conduct will be treated seriously and in line with student and staff disciplinary codes and procedures, or other college protocols as appropriate.

Where conduct is found to be unacceptable, the College will normally deal with the matter internally, however where conduct is considered to be illegal, the College will report the matter to the police.

4.4 Communications and Social Networking

i The College recognises the role that social networking and other communication technologies holds within modern student life and learning and teaching practice. As such, these technologies are used within the College and made appropriately available to staff and students within the institutional ICT systems and networks.

In using these technologies, including email, mobile phones, social networking sites, games consoles, chatrooms, video conferencing and web cameras, the College requires all users to adhere to the practice detailed within the Acceptable Use Policy.

All staff members using social networking sites as tools through which to communicate with students must only do so on a professional basis.

Title: E-Safety Policy
Version/Status: 1.2, Final
Approved By/Date: CMT, 08/2011

Effective Publication Date: August 2011

Owner: Depute Principal, Academic
Lead Author: Head of Student Experience
Student Services Manager
Review Timing/Date: 5 Years/2016/17

Therefore, any groups that are set up under the Perth College UHI name must only be done so using a college e-mail account, and in line with the staff Code of Conduct detailed within the Safeguarding Policy. As such, staff must not become friends with students within social networking or other virtual environments, and must not share personal information with students. All communications should be made in such a way that the professional position of the staff member(s) is not compromised and the relationship with the student(s) remains appropriate in terms of professional boundaries.

- ii Where a staff member chooses to join a group set up within a social networking site by a student, the staff member must only do so using their designated college e-mail account and having established that the nature and purpose of the group are appropriate in terms of the professional relationship.
- iii Since social networking technologies are not College systems, and the use of these technologies is optional, it is essential that where such systems are used by staff for the purposes of communication or discussion with students, that appropriate steps are taken to ensure that any student who chooses not to register with or use the technologies is not disadvantaged in their learning or overall student experience.

4.5 Use of Images and Video

The use of images or photographs within the College's learning and teaching and other activities is acceptable where there is no breach of copyright or other rights of another person. This includes images downloaded from the internet and images belonging to staff or students.

Photographs of activities and people on the College premises are considered carefully in terms of individual privacy and equality and diversity, and the consent of individuals pictured is sought prior to publication.

The potential risks of sharing personal images and photographs within social networking sites, and other areas of the internet for example are particularly relevant to e-safety. As such the College provides information, advice and training to students and staff on these risks and steps that can be taken to protect personal images and photographs as well as other personal information.

4.6 Personal Data

Perth College UHI collects and stores personal data such as names, dates of birth, email addresses, of students and staff regularly in line with operational requirements. The College has in place arrangements to ensure the secure and confidential storage of personal information, and that information is only shared appropriately and in line with Data Protection legislation and guidance.

All staff are required to gather, store and use students' personal information appropriately.

Title: E-Safety Policy
Version/Status: 1.2, Final
Approved By/Date: CMT, 08/2011
Effective Publication Date: August 2011

Owner: Depute Principal, Academic
Lead Author: Head of Student Experience
Student Services Manager
Review Timing/Date: 5 Years/2016/17

4.7 **Education and Training**

While this Policy aims to ensure that ICT systems and resources are used appropriately and safely within the College, it is impossible to eliminate all risks. However, the College considers it to be an essential part of its approach to e-safety, for staff and students to be equipped with the knowledge and skills to operate safely within the range of technologies that is available. Through training and education, the College will provide staff and students with information and skills to enable them to identify risks independently and take steps to manage them effectively.

A range of CPD opportunities will be provided to staff on the topic of e-safety, and similarly, students will be offered both information and training opportunities at various points throughout their period of study with the College.

4.8 **Incident Monitoring and Management**

Perth College UHI will monitor the impact and effectiveness of this policy and will respond to any reported e-safety incident swiftly, and in line with other relevant policies and procedures such as the Acceptable Use Policy and the Safeguarding Policy and Procedure. The College will act immediately to prevent or minimise, as far as reasonably possible, any harm or further harm from occurring.

Students will be made aware that should they wish to report an incident, they can do so to their Personal Academic Tutor or Head of Curriculum. Where a member of staff wishes to report an incident, they will be able to do so through their line manager.

Following any incident, the College will take steps to address the matter thoroughly and appropriately and action may include the involvement of external agencies as necessary.

In order to ensure a fully appropriate and comprehensive response, serious incidents will be dealt with by or in conjunction with the Senior Management Team.

5 **Responsibilities**

- 5.1 The Depute Principal, Academic will have overall responsibility for the Policy and its implementation.
- 5.2 The Chief Operating Officer is responsible for managing the ICT infrastructure of the College and the security of the data and user information held within College systems as detailed in the ICT Security Policy.
- 5.3 The Head of Student Experience is responsible for managing the Safeguarding arrangements within the College, including the Policy and Procedure and as such, is responsible for ensure appropriate linkage between the E-Safety and the Safeguarding Policies. Review and updating of the policy will also be undertaken by the Head of Student Services

Title: E-Safety Policy

Version/Status: 1.2, Final

Approved By/Date: CMT, 08/2011

Effective Publication Date: August 2011

Owner: Depute Principal, Academic

Lead Author: Head of Student Experience
Student Services Manager

Review Timing/Date: 5 Years/2016/17

- 5.4 The Chief Operating Officer and the Head of Student Experience are jointly responsible for monitoring the impact of the policy and for coordinating responses to any e-safety incidents or concerns.
- 5.3 The Chief Operating Officer is responsible for the co-ordination and delivery of learning materials relevant to e-safety, for staff and student use.
- 5.4 All staff members are responsible for ensuring that their professional practice within their role at the College is compliant with the content of this and other linked policies.
- 5.5 Students are responsible for ensuring that their use of College systems is compliant with the content of this and other linked policies.
- 5.6 Quality approval checking of the policy is the responsibility of the Quality Manager who will arrange for the policy to be posted on the web.

6 **Linked Policies/Related Documents**

- 6.1 Perth College UHI ICT Acceptable Use Policy
- 6.2 Perth College UHI ICT Security Policy
- 6.3 Perth College UHI Safeguarding Policy and Procedure
- 6.4 Perth College UHI Data Protection Policy and Guidelines
- 6.5 Perth College UHI Staff Disciplinary Procedure
- 6.6 Perth College UHI Student Disciplinary Procedure

7 **Relevant Legislation**

- 7.1 Protection of Children (Scotland) Act (2003)
- 7.2 Adult Support and Protection (Scotland) Act (2007)
- 7.3 The Data Protection Act (1998)
- 7.4 Copyright, Designs and Patents Act (1988)
- 7.5 Computer Misuse Act (1990)
- 7.6 Regulation of Investigatory Powers Act (2000)
- 7.7 Freedom of Information Act (2000)
- 7.8 Human Rights Act (1998)

Title: E-Safety Policy
Version/Status: 1.2, Final
Approved By/Date: CMT, 08/2011
Effective Publication Date: August 2011

Owner: Depute Principal, Academic
Lead Author: Head of Student Experience
Student Services Manager
Review Timing/Date: 5 Years/2016/17