Information Services
Policy Document

UNIVERSITY OF CUMBRIA

E-SAFETY POLICY

Information Services

NB. This policy is available on the University of Cumbria website and it should be noted that any printed copies are uncontrolled and cannot be guaranteed to constitute the current version of the policy.

POLICY SCHEDULE	
Policy title	E-Safety Policy
Policy owner	Director of Information Services, Colin Coghill
Policy lead contact	Head of Technology Services, Stephen Murray
Policy Number	POL004
Approving body	University Management Team
Date of approval	25/04/2012
Date of implementation	25/04/2012
Version no.	1.3
Related Guidelines, Procedures, Codes of Practice etc.	JANET (UK) Acceptable Usage Policy - covers all users of the JANET network. Safeguarding Vulnerable Groups Information Security Policy Social Media Policy HM Government Prevent Duty Guidance 2015
Review interval	Annual

Document Information

Scope

This policy applies to all staff and students at the university.

It also applies to partners, visitors and guests of the university using the university infrastructure.

Document history

Version	Date	Author	Comments
0.1	03/12/2010	Peter Hurst	
0.2	03/03/2011	Peter Hurst	
0.3	05/04/2011	Peter Hurst	
0.4	04/07/2011	Colin Coghill	Academic enabling. Policy separate from implementation. Remove FE
0.5	23/09/2011	Colin Coghill	Changes after ITSG
1.0	25/04/2012	Colin Coghill	Changes after UMT and final approval
1.2	20/5/2015	Peter Hurst	Incorporating HMG Prevent Guidance 2015
1.3	02/08/16	Carne Burke	Annual review and minor updates including new Head of Technology Services
1.4	02/03/2017	Carne Burke	Review and minor updates
1.5	18/04/2018	Stephen Young	Service name update

Contents

1. Introduction

The university is committed to ensuring the wellbeing and safety of all our staff, students and partners, and this extends to the use of IT resources. The aim of this policy is to ensure *users* are able to use our IT safely.

The university must also ensure that IT resources are used according to legal, regulatory and contractual requirements. However, we are a university, and IT users must be able to access electronic information to further their scholarly research and studies and our controls must reflect this.

This policy is an expansion of the University of Cumbria Information Security Policy.

This Policy needs to be viewed distinctly from its implementation: the principles and approach are held in the Policy; the details of systems, technologies, processes and thresholds are described in implementation procedures and guidelines. It is getting these levels and technologies right that will ultimately affect the ease of use of IT resources.

2. Policy Requirements

An E-Safety Policy needs to cover risks which include:

- Individuals may be harmed by inappropriate material accessed via the web or other electronic means. The definition of 'inappropriate' will depend on the point of view and the implementation approach taken. University committees will guide the Policy on this.
- Individuals may be the target of promoting extremism, terrorism or 'cyber bullying' on social networks, email, etc.
- There is a risk of hacking, data loss and generating undesirable content from university systems, such as 'spam' emails or website defacement.
- Potential Health and Safety legislation breaches.
- Student retention.
- Adverse audits.
- Financial loss through litigation or time loss.
- Reputational loss to the university, from security or wellbeing issues.
- The university has a contractual duty, as part of its agreement to connect to the JANET network, to be able to track and report on suspicious network traffic, virus infection or abuse.
- The university has a legal responsibility to be able to provide suitable logs to law enforcement agencies.

This policy informs all the implementation measures in place intended to promote the health, safety and welfare of all users within the context of E-Safety. Systems are designed to safeguard users while ensuring academic freedom with mechanisms to allow exceptions where appropriate.

The policy is also intended to assure staff, students, learners and parents, guardians or carers that the university takes e-safety seriously.

3. Policy Principles

The policy outlines the technical measures that protect the university and its staff, students, visitors and partners from unintentional harm. The university promotes safe use of the internet in a number of ways:

Secure management of university computer resources:-

- University firewalls prevent peer-peer programs and insecure protocols to protect data and data leakage.
- Only secure and authorised devices are permitted to access the university email system.
- Software is installed according to licensing and security requirements.
- Web publishing guidelines prevent the gathering of personal information.
- Anti-virus software is used to scan computers, internet traffic and emails to automatically block the majority of damaging programs.
- Network traffic is scanned to prevent viruses and other 'malware' entering university systems.
- Emails are automatically scanned to remove the majority of unwanted spam content according to manufacturer/service provider standards.
- Web Protection Systems (WPS) automatically attempt to categorise unknown websites based on content and scans for malware.
-

4. Risk Management Statement

The risks associated with not applying measures to safeguard users of IT are referenced in Section 2 above. The management of these risks starts with the adoption of this policy and then its implementation using appropriate technology, process and communication solutions.

5. Roles and Responsibilities

Everyone in the university has some responsibility for e-safety.

- All users of electronic resources should also be aware of their own behaviour and take care that it is not upsetting or hurting someone else, even accidentally.
- All users have a responsibility to report inappropriately classified material. No automated process will be 100% effective – being allowed a resource does not automatically make it safe.
- Service managers and tutors should ensure the intentions of the policy are carried out and support awareness-raising with students and learners.
- Academic staff will need to make Information Services aware of groups requiring exceptional access.
- Information Services oversees the university's policy for e-safety and provides the technological and process implementation of the E-Safety Policy.
- The IT Service Desk should always be the first point of contact for exemptions for sites, individuals or groups.

6. Inappropriate Use Complaints

If a complaint is received that a student, learner or staff member is misusing university IT resources, or is being bullied or harassed, then actions may be taken using the appropriate procedures.

- Complaints about the behaviour of a student or learner may be considered under the Student Code of Conduct & Adjudication Procedure.

- Complaints about the behaviour of a staff member will be referred to Human Resources for consideration.

Appendix A – Web Filtering Implementation

Web protection is designed to prevent inadvertent unsafe or illegal access, damage or embarrassment. Any restrictions are designed to block the majority of sites considered inappropriate or unacceptable, not to restrict academic freedom.

It is acknowledged that the definition of inappropriate or unacceptable will vary according to an individual or a group. Therefore, the implementation of this Policy must be based on agreed university values.

The main categories addressed are:

- drugs - For example, websites that sell illegal/controlled substances, promote substance abuse or sell related paraphernalia.
- gambling – For example, on/offline gambling and websites that promote gambling skills and practice.
- hate and discrimination - For example, websites that promote aggressive, degrading, or abusive opinions about any section of the population on the basis of an individual's race, religion, gender, age, nationality, physical disability, sexual preferences or any other lifestyle choice.
- pornography and adult material - For example, websites containing sexually explicit content.
- violence - For example, websites that display or promote content related to violence against humans or animals.
- terrorism and extremism - For example, websites promoting terrorist activities, radicalisation or extremism.

The university uses a service provider to automatically prevent access to websites in the above categories known to be a problem or known to be illegal. As all network access is treated equally, the minimum tolerance level for protection has to be provided to adequately protect our most vulnerable groups or statutory requirements.

<u>Exemptions</u>

Where academic or business needs conflict with the university implementation, exceptions can be made for an individual, a group or named sites. The exception process is simple and the authorisation belongs to the academic or service leader, not Information Services. The IT Service Desk should always be the first point of contact for exemptions for sites, individuals or groups.