Lews Castle College UHI IT Policy Statement

Section 1 - Computer Ethics, Copyrights and Intellectual Property

1.1 Staff and students are prohibited from making copies of any programs stored on any college desktop or server.

1.2 Only ICT staff are authorised to make backup copies of software for which the college is licenced, only for the purpose of retaining a copy of the software to protect the original data and purpose for which the software was purchased.

1.3 Users of Lews Castle College UHI resources must understand that it is breach of copyright to use text, images, sounds, video, scripts and other objects on and off web pages without the appropriate credit and permission from the owners.

1.4 Computer software is protected by UK and International Copyright law and is subject to criminal prosecution which includes heavy fines and imprisonment.

1.5 Lews Castle College UHI ICT system administrators have the right to protect their Intranet and Internet facilities to ensure that they abide by the terms and conditions of the Joint Academic Network agreement (JANET).

Section 2 - Computing Rights and Responsibilities

2.1 Computers and networks within the University of the Highlands & Islands (including Lews Castle College UHI and its Learning centres) can provide access to teaching materials on and off campus, therefore regarded as a privilege and must not be abused.

2.2 ICT system administrators reserve the right to firewall ports to protect the integrity of the college’s network and resources from harmful attacks.

2.3 Under no circumstances must food or drink be brought into any computing/ICT resource area within the college or Learning centres.

2.4 Electronic mail is an extremely powerful tool and must not be abused by spamming or sending commercial or unacceptable materials to any user on the University of the Highlands & Islands Network, JANET Network, or any other internetworked system whilst operating from the college’s network.

2.5 Anti-Virus Software is there for the user’s protection therefore settings must not be tampered with.

2.6 ICT System administrators reserve the right to deny users access to rooms or resources in the event of a system breach.

2.7 Personal storage space will be scanned for viruses and illegal content, any software deemed to be illegal may result in disciplinary action taken against offenders.

Section 3 - Legal Issues

3.1 Users have the right to access information held about themselves on computer files as stated in the Data Protection Act 1998.

3.2 Users may be held accountable for their conduct while operating any college ICT resource.

3.3 Complaints alleging misuse of computing and networking resources will be directed to the ICT Systems Manager or any authorised member of staff who would be responsible for taking appropriate disciplinary action.

3.4 Any user found trying to hack/crack or breach any college, University of the Highlands & Islands computer system or soliciting with hackers/crackers will be immediately banned from using any of the college’s computing resources in the future and risk prosecution under the Computer Misuse Act 1990 (UK).
Section 4 - CCTV (Closed Circuit Television)

4.1 Users must be aware they are monitored by CCTV systems for the purposes of Security and Safety. Areas that are monitored by CCTV will be recorded and held on magnetic media (Videotape) for a period of time.

Section 5 - Examples of Misuse of Computing and Network Resources

Examples of misuse include, but are not limited to, the activities in the following list *

5.1 Giving anyone your username/password(s) or access to any of your Lews Castle College UHI computing accounts.
5.2 Using a computer account or obtaining a password for a computer account that you are not authorized to use.
5.3 Deliberately viewing or creating obscene or indecent material (include, but are not limited to that which portrays sex, nudity, violence or suffering in a gratuitous manner).
5.4 Knowingly install third party software onto any computer system or network within the college.
5.5 Using Lews Castle College UHI computing resources for commercial activities in violation of the College’s policy.
5.6 Using copyrighted text, images, sounds, video without proper credit to and permission from the owner.
5.7 Using electronic mail to harass others and/or to pass chain letters to others.
5.8 Sending Selective Promotion Advertising Mail (SPAM) to large groups of users, either on or off campus.
5.9 Deliberately wasting computing resources and/or supplies.
5.10 Attempting to monitor or tamper with another user’s account.
5.11 Reading, copying, changing, or deleting another user's files or software without the owner's explicit consent.
5.12 Using any Lews Castle College UHI computing resource to gain unauthorised access to any computer system.
5.13 Revealing confidential information obtained from administrative data systems to unauthorised people or groups.
5.14 Attempting to circumvent data protection schemes or uncover security loopholes.
5.15 Violating terms of applicable software licensing agreements or copyright laws.
5.16 Knowingly running or installing on any computer system or network, or giving to another user, a program intended to damage or to place excessive load on a computer system or network. This includes but is not limited to programs known as computer viruses, Trojans, and worms.

* Except when authorised by the ICT Systems Manager for security or performance testing.

Section 6 – Students’ Personal Data

6.1 Electronic backup facilities can be accessed by contacting the IT Support Department.
6.2 All electronic data including personal storage space and email shall be deleted 30 days after completion of course or program of study.
6.3 Applications for the extension of the 30 day period will be considered on receipt of a written explanation to be lodged with the ICT Systems Manager, no later than 7 days prior to completion of your course or program of study at Lews Castle College UHI.
Section 7 – Password Policy

7.1 All system-level passwords (e.g., root, enable, server admin, application administration accounts, etc.) must be changed on at least a quarterly basis.

7.2 All production system-level passwords must be party of the administered global password management database.

7.3 All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every four months.

7.4 User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.

7.5 Passwords must not be inserted into email messages or other forms of electronic communication.

7.6 All user-level and system-level passwords must conform to the guidelines described below.

7.7 Strong passwords have the following characteristics:
   - Contain both upper and lower case characters (e.g., a-z, A-Z)
   - Have digits and punctuation characters as well as letters (e.g., 0-9, !@#$%^&*()_+~-=\[]:";'<>?,./)
   - Are at least eight alpha-numeric characters long
   - Are not in any language, slang, dialect, jargon, etc.
   - Are not based on personal information, names of family, etc.

7.8 Passwords should never be written down or stored on-line. Try to create passwords that can easily be remembered.

Section 8 – Elevated User Rights (EUR)

8.1 Because running with EUR always adds risk of data loss or computer virus or machine malfunction, IT Service will seek to keep numbers running with EUR to a minimum and therefore not all requests will necessarily be met.

8.2 Generally EUR, if granted, will be for one staff member and one machine. EUR for one user over multiple machines will only be granted in truly exceptional circumstance due to security risk and privacy concerns.

For Further Information Contact:
Danny Richardson
ICT Systems Manager
Tel: 01851 770262
Email: danny.richardson@uhi.ac.uk

1 Please see Lewis Castle College UHI Password Policy Statement for a full explanation of the password policy.