University of the
Highlands and Islands
West Highland College

Oilthigh na Gàidhealtachd
agus nan Eilean
Colaiste na Gàidhealtachd an Iar

ICT Security Policy

ELT manager	Director of Finance & Corporate Services
Responsible officer	Facilities Manager
Date first approved by BoM	12 April 2016
First Review Date	April 2019
Date review approved by BoM	
Next Review Date	
Equality impact assessment	
Further information (where relevant)	

Reviewer	Date	Review Action/Impact	BoM

ICT Security Policy (Part A)

1.0 Purpose

West Highland College UHI is committed to protecting the personal data of members of staff and students, protecting other key college information systems, and developing the skills and knowledge of our staff and students to support them in maintaining their on-line safety. This policy is to make staff and students aware of their responsibilities in respect of ICT security.

2.0 Scope

This policy is applicable to all data held within ICT systems including but not restricted to: desktop computers, network servers, portable equipment and electronic data.

3.0 Definitions

The College is defined as staff and students.

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. ICT consists of IT as well as telephony, broadcast media, and all types of audio and video processing and transmission.

Information takes many forms and includes: data stored on computers; transmitted across networks; printed out or written on paper; sent by e-mail or fax; stored on tapes, CDs or any other media; and spoken in conversation or over the telephone.

The College's key systems are:

- Finance.
- Intranet services.
- Website services.
- Human Resources.
- Payroll.

In addition the following systems are available via UHI:

- E-mail System.
- Virtual Learning Environment.
- Student Records.
- Library Management System

4.0 Key Principles

The College's security measures must operate within the following framework:

- Confidentiality – knowing that key data and information can be accessed only by authorised personnel;

- Integrity – ensuring that key data and information is safe, accurate and up-to-date and has not been deliberately or inadvertently modified from a previously approved version;

- Availability – knowing that the key data and information can always be accessed; and;

- Safety – ensuring that students and staff are equipped with the knowledge and understanding to maintain their on-line safety.

The College is required to meet its statutory responsibilities in terms of managing data and information. These responsibilities are mainly covered by the legislation listed in Section 7 of this document.

5.0 Responsibilities

5.1 **Student Responsibilities**

The following policies/documents should be read in conjunction with this policy:

- ICT Acceptable Use Policy for Staff and Students
- E-Safety Policy
- Social Media Policy
- Netiquette Protocol
- West Highland College ICT Guide for Staff and Students
- UHI Student Charter
- Safeguarding Policy and Procedure: Child and Vulnerable Adult Protection

5.2 **Employee Responsibilities**

The following policies should be read in conjunction with this policy:

- ICT Acceptable Use Policy for Staff and Students
- E-Safety Policy
- Social Media Policy
- Netiquette Protocol
- Data Protection Policy
- Freedom of Information Model Publication Scheme
- West Highland College ICT Guide for Staff and Students
- Safeguarding Policy and Procedure: Child and Vulnerable Adult Protection

All College staff who use or come into contact with, confidential records are individually responsible for their safekeeping.

Staff should be aware of their contractual and legal confidentiality obligations.

General internet access carries with it a security risk of downloading viruses or programmes that can look around a network and infiltrate password security systems. This information can then be sent back to the originator of the programme in order to allow them unauthorised access to the College's systems.
Employees must use care when transferring data between their home PC and College network.
All home PCs which are used for the manipulation of College data must have a current virus checker.

5.3 **Management Responsibilities**

The Director of Finance and Corporate Services is responsible for providing help and guidance on all matters relating to information security.

The Human Resources Manager is responsible for providing up-to-date information on data protection and freedom of information matters.

The Student Services Manager is responsible for providing up-to-date information on safeguarding requirements and current issues relating to on-line safety.

Quality approval check of the policy is the responsibility of the Estates and Facilities Manager who will arrange for the policy to be posted on the web.

All Managers are responsible for ensuring compliance with this policy.

Key management responsibilities include:

- Compliance with data subject enquiry procedures (as required by the Data Protection Act 1988);

- Ensuring IT media and equipment disposal is properly authorised and securely undertaken;

- Ensuring members of staff are instructed in their security responsibilities, including implementing password control;

- Ensuring members of staff are aware of the confidentiality clauses in their contract of employment;

- Ensuring that the relevant managers are advised immediately about staff changes affecting computer access.

6.0 Linked Policies/Related Documents

- Data Protection Policy and Guidelines.
- E-Safety Policy

- Social Media Policy
- Netiquette Protocol
- Freedom of Information Model Publication Scheme.
- ICT Acceptable Use Policy for Staff and Students.
- West Highland College ICT Guide for Staff and Students.
- Safeguarding Policy and Procedure: Child and Vulnerable Adult Protection
- Getting it Right for Every Child (Scottish Executive, 2005).
- Records Management Policy.

7.0 **Relevant Legislation**

- The Data Protection Act (1998).
- Copyright, Designs and Patents Act (1988).
- Computer Misuse Act (1990).
- Regulation of Investigatory Powers Act (2000).
- Freedom of Information Act (2000).
- Human Rights Act (1998).
- Protection of Children (Scotland) Act (2003).
- Adult Support and Protection (Scotland) Act (2007).

ICT Security Policy (Part B)

The following paragraphs apply to the key principles as follows:

1.0 Confidentiality

1.1 Sharing Data and Data Transfer

The College works with partner organisations (such as SQA, City and Guilds, and Skills Development Scotland) which all have a legitimate role to play in delivering education and training. These partnerships might require the transfer of personal data between the partners. Personal data shall include both hard copy as well as electronic format.

The College has a duty to comply with the Data Protection Act. The transfer of personal data to a partner organisation must, therefore, be pre-authorised by the Human Resources Manager for staff data and the Vice Principal (Academic Affairs) for student data

1.2 Access Control

1.2.1 Students

Student accounts are rendered inactive at the end of their course, whilst continuing students' accounts remain active until such times as they elect not to return or withdraw.

1.2.2 Staff

Staff, students and contractors should only access systems for which they are authorised. Access privileges will be modified/removed, as appropriate, when an individual changes job/leaves.

All key systems should be adequately documented by the relevant systems manager. Such documentation should be kept up to date so that it matches the state of the system at all times. System documentation, including manuals, should be physically secured when not in use.

The College reserves the right for appropriately authorised staff to examine any data including personal data held on College systems or, when operationally necessary, for example to give supervised access to a private account to a line manager or colleague. Certain staff within the College have been authorised to examine files, emails and data within individual accounts, but will only do so when operationally necessary.

When a member of staff leaves the employment of the College their user account(s) shall be ended as part of the termination action carried out by the Human Resources department. Thereafter, the College has the right to access the account for operational reasons and for the continuing delivery of services.

Prior to an employee's termination of contract, line managers should ensure that:

- All IT assets are returned to the College (eg laptops, mobile devices).
- The employee does not inappropriately wipe or delete information from hard disks. If the circumstances of leaving make this likely then access rights should be restricted to avoid damage to College information and equipment.

1.2.3 Visitors

No external party shall be given access to any of the College's key systems unless that party has been formally authorised by an appropriate Manager. Prior to access being granted they will be required to sign (electronically or otherwise) the College's ICT Acceptable Use Policy.

If temporary passwords need to be issued to allow access to confidential systems these need to be disabled when the visitor has left. Visitors should not be afforded an opportunity to casually view computer screens or printed documents produced by any information system without authorisation from the relevant functional manager.

1.3 Password Management

Passwords are the responsibility of individual users and must be kept confidential. The passing of an authorised password to someone unauthorised in order to gain access to an information system may be a disciplinary offence.

Whilst we are unable to enforce password change all users should be encouraged to change their network passwords at three monthly intervals.

2.0 Integrity

2.1 Virus Protection

Viruses are one of the greatest threats to the College's computer systems. Anti-virus measures reduce the risks of damage to the College's PCs and network.

The College seeks to minimise the risks of computer viruses through education, good practice/procedures. To this end, staff and student PCs are configured in such a way as to block the unauthorised installation of software.

Anti-virus protection software must be installed on all of the College PCs. If a member of staff believes that his/her PC is not protected then he/she must contact the ICT Helpdesk immediately. Similarly, if a member of staff is unsure whether the installed virus protection software is being automatically updated he/she must contact the ICT Helpdesk immediately. Users should report any viruses detected/suspected on their equipment to the ICT Helpdesk immediately.

2.2 Software and Information Protection

All student and staff PCs shall be controlled to prevent the installation of malicious or fraudulent software/code.

The loading and use of unlicensed software on College computing equipment is not allowed. All staff and students must comply with the Copyright, Designs and Patents Act (1988). This states that it is illegal to copy and use software without the copyright owner's consent or the appropriate licence to prove the software was legally acquired. Any breach of software copyright may result in personal litigation by the software author or distributor and may be the basis for disciplinary action under the College Disciplinary Procedures.

The installation of leisure software (eg games) onto computing equipment owned by the College is not allowed.

2.3 Key Information and Business Systems

Key systems shall be protected by physical security and user access control measures and data storage and backup.

All hard copy staff, student, financial, research and corporate records should be stored in a secure area and not left in an unattended, unlocked room. They should only be retained for the minimum length of time that they are absolutely required. Access to key IT systems and key data and information will only be granted on a need to know basis. Segregation of duties between operations and development environment shall be maintained for critical systems. Permanent and full access to live operating environments will be identified and action taken to implement split functional controls where appropriate.

Information security awareness training and/or instruction will be made available to staff as part of the College's induction process.

2.4 Physical Security

Controls shall be implemented as appropriate to prevent unauthorised access to, interference with, or damage to, the College's IT systems. College systems and networks will be protected by suitable physical, technical, procedural and environmental security controls.

File servers that hold or process critical and/or sensitive data will be located in physically secured areas. Access to these facilities shall be controlled.

PCs or terminals should be secured by password access control when not in use.

2.5 Security of Data

Users of IT facilities are responsible for safeguarding key data by ensuring that desktop machines are not left logged-on when unattended and that portable equipment is not exposed to opportunistic theft.

Users should log off or lock terminals or PCs when leaving them unattended. Inactive PCs or terminals shall be set to time out after a pre-set period of inactivity. The time-out delay should reflect the security risks of this area.

Local file servers shall be protected by UPS backup to the mains electricity supply.

2.6 Portable Equipment

Users of portable equipment belonging to the College are responsible for the security of the hardware and the information it holds at all times on or off College property. The equipment should only be used by the College staff to which it is issued. All of the policy statements regarding the use of software and games apply equally to users of portable equipment belonging to the College.

2.7 Equipment, Media and Data Disposal

If a machine has ever been used to process personal data then any storage media should be disposed of only after reliable precautions to destroy the data have been taken. Therefore, disposal should only be arranged by contacting the Estates and Facilities Manager.

2.8 Network Security

It is the responsibility of the Estates and Facilities Manager to ensure that access rights and control of traffic on all College networks are correctly maintained.

It is the responsibility of the Estates and Facilities Manager to ensure that data communications to remote networks and computing facilities do not compromise the security of the College systems.

All communications cabling will be arranged by Estates and Facilities and cannot be authorised without their involvement.

Software installation by any personnel other that ICT Support is not permitted. A Helpdesk Service Request should be completed when requesting software installation. The Estates and Facilities Manager will retain all software licences.

All users must take appropriate precautions to ensure that another user cannot gain unauthorised access using their equipment. In particular, equipment should not be left unattended unless it has a password protected screen saver or menu or it has been logged out.

2.9 Hardware and Software Acquisition

All hardware and software must be authorised and purchased through the Estates and Facilities Manager.

Software installation by any personnel other than ICT Support Centre Managers to whom local admin rights have been approved is not permitted.

All hardware will be installed onto college systems by ICT Support staff only.

The placement, re-positioning and removal of computer equipment can only be authorised by, and carried out under instruction from the Estates and Facilities Manager or IT Support.

3.0 Safeguarding Students

The College will use a range of means to tell students about on-line safety and offer opportunities for them to learn more and develop skills throughout the duration of their course of study. This includes, but is not limited to:

- Embedding learning opportunities in mainstream curriculum;
- Induction sessions;
- Tutorials;
- Student advising;

4.0 Incident Management

Users must contact the ICT Helpdesk if they are aware of, or suspect a security breach.

Any computer or mobile device that is perceived to be placing the integrity of the College's ICT network at risk will be disconnected.

5.0 Availability/Inventory

5.1 Data Storage and Backup

All electronic data will be held on a network resource so that it is backed up through a routine managed process. Care should be taken storing information on a PC hard drive as data may not be retrievable in the effect of equipment.

Backup media containing key data must be stored off-site or a sufficient distance from the original source so as to remain available in the event of the live system being lost through a major localised incident.

Recovery data should be sufficient to provide an adequate level of service in the event of an emergency and should be regularly tested.

5.2 Equipment Inventory

An inventory of all computer equipment and software will be maintained.

The Estates and Facilities Manager has responsibility for the inventories on all of the college sites.

5.3 Software register

An up-to-date register of all proprietary software will be maintained to ensure that the College is aware of its assets and the licence conditions are adhered to. This register will be maintained by the Estates and Facilities Manager for all college installed software applications.

All hardware and software must be authorised and purchased through the Estates and Facilities Department

6.0 **Linked Policies/Related Documents:**

- Data Protection Policy and Guidelines.
- E-Safety Policy
- Social Media Policy
- Netiquette Protocol
- Freedom of Information Model Publication Scheme.
- ICT Acceptable Use Policy for Staff and Students.
- West Highland College ICT Guide for Staff and Students.
- Safeguarding Policy and Procedure: Child and Vulnerable Adult Protection
- Getting it Right for Every Child (Scottish Executive, 2005).
- Records Management Policy.

7.0 Relevant Legislation:

- Copyright, Designs and Patents Act 1988

- Malicious Communications Act 1988
- Computer Misuse Act 1990
- Data Protection Act 2003
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000
- Freedom of Information (Scotland) Act 2002
- The Bribery Act 2010