Information Technology (IT) Security Policy

Authors: Bill Dunsmuir – Head of Information Systems and Digital Infrastructure
Brian Smillie – Digital Infrastructure (DI) Manager

Impact Assessment Date: 18 November 2022

Date: 17 January 2023

Review: December 2025

Contents

History of Changes

Version	Description of Change	Authorised by	Date
1.1	Minor changes to original policy and procedure	Simon Earp	18/11/2022
1.2	Removal of reference to safeguarding and online safety, covered in separate policies	Simon Earp	30/01/2023

Statement of Inclusiveness

West Lothian College is an inclusive organisation and all policies, procedures, strategies, plans, provisions, criteria, functions, practices and activities, including decisions and the delivery of services are assessed to consider the impact on staff and students covered by the Equalities Act 2010 by the completion of an Equalities Impact Assessment (EIA). Protected characteristics are defined as age, disability, gender reassignment, marriage or civil partnership (in employment only), pregnancy and maternity, race, religion or belief, sex, sexual orientation.

1 Introduction

West Lothian College is committed to protecting its computer systems, personal data, college information systems and the online safety of staff, students and guests as well as meeting its statutory responsibilities in terms of managing data and information.

Information takes many forms and includes data stored on computers, laptops, tablets, phones, or any other digital device; transmitted across networks; sent by e-mail or fax; and stored on USB drives or any other media.

IT consists of all technical means used to handle digital information and aid communication, including computer and network hardware, software and data and information management. This policy is also applicable to all data held within college IT systems including but not restricted to desktop computers, network servers, mobile equipment, telephony, portable equipment, and electronic data.

2 Scope

This policy applies to students and all college employees including: staff both full and part-time, seasonal, temporary, casual, interim, student workers, interns and volunteer employees and covers all offsite locations.

3 Supporting Policies

This overarching policy is supported and extended by the following topical policies:

- Remote Access Policy
- Email Computer Network Acceptable Use Policy

These policies can be found Staff Zone - Policies - All Documents (sharepoint.com)

4 Key Principles

4.1 CIA Security Triad

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 online safety.

5 General Policy

5.1 Anti-virus

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, portable devices, and network. The college seeks to minimise the risks of computer viruses through education, good practice/procedures.

- Staff and student PCs and portable devices must be 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, laptops, and servers. Anti-virus should be installed on portable devices wherever reasonable.
- If staff or students believe that their college PC is not protected then they must contact the Helpdesk immediately.
- If staff or students are unsure whether the installed virus protection software is being automatically updated, they must contact the Helpdesk immediately.
- Staff or students should report any viruses detected/suspected on their equipment immediately by logging a call via the Helpdesk.

5.2 Software Installation and Licensing

Software installation:

- The loading and use of unlicensed software on college computing equipment is not allowed.
- The installation of leisure software (e.g. games) onto computing equipment owned by the college is not allowed.
- Software installation by any person other than IT Services is not permitted.
- Requests for installs should be generated through the Helpdesk.

Software licensing:

- The DI Manager will be responsible for retaining all software licences used in the college.
- 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.
- Logging onto multiple devices to allow others to download software is strictly forbidden.

6 Staff Policy

6.1 Data Protection and Data Handling

- Staff should be aware of their contractual and legal confidentiality obligations.
- All college staff who use or come into contact with, confidential records are individually responsible for their safekeeping.

6.2 Staff Leaver

- 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 (HR) department.
- Prior to an employee's termination of contract, HR will ask the employee to ensure that:

    - All IT assets are returned to the college (e.g. 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.
    - All relevant information, contacts & appointments associated with the role should be passed onto the department manager prior to termination.
    - Email accounts are deleted after 30 days of being disabled.

- After termination, the college has the right to access the staff member’s accounts for operational reasons and for the continuing delivery of services.

6.3 System Management

- All key systems should be adequately documented by the system's owner.
- Such documentation should be kept up to date so that it matches the state of the system at all times.
- Key IT systems shall be protected by physical security and user access control measures and data storage and backup.
- Physical access controls shall be implemented 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 and limited to IT Services only.
- Key IT systems shall be protected by an uninterruptable power supply (UPS) in case of power failure.

6.4 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. Information should not be held solely on a PC hard drive or other local device storage.
- Backup media containing key data must be stored off-site or a sufficient distance from the 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 and recovery time in the event of an emergency and should be regularly tested.

6.5 Secure Media Disposal

- If a machine has ever been used to store or process personal data or college-sensitive data then any storage media should be disposed of only after reliable precautions to destroy the data have been taken.
- All media, including removable media, that has been used to store personal data or college-sensitive data should be disposed of only after reliable precautions to destroy the data have been taken
- Disposal should only be arranged by contacting the IT Helpdesk.

6.6 Network and Infrastructure Security

- It is the responsibility of the DI 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 the IT Services and cannot be authorised without their involvement.

6.7 Hardware and Software Acquisition

- All hardware and software must be discussed and approved by the DI Team prior to raising purchase orders.
- Any orders raised will be passed for authorisation from the DI Team.
- Software installation by any college personnel other than IT Services is not permitted.
- All hardware will be installed onto college systems by IT Services staff only.
- The placement, repositioning and removal of computer equipment can only be authorised by and carried out under instruction from the DI Team**.**

Equipment Inventory

- An inventory of all computer equipment will be maintained.
- The Digital Infrastructure team have responsibility for the inventories on all of the college sites.

Software Register

- An up-to-date register of all 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 Digital Infrastructure team for all college installed software applications.

6.8 Security Awareness and Education

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

    - Induction sessions
    - Moodle
    - Lecturer input
    - Student Association

- The college will train employees in cyber security skills and awareness to prepare them for inevitable attacks and to create a culture of cyber safety.

    - Mandatory employee cyber security training will be delivered as part of the Staff Development Programme, with training completion tracked and reported on by that programme.
    - Year-round discretionary cyber awareness and tips are provided by the Digital Infrastructure team through various methods to encourage engagement and participation with the material.

7 College Management Responsibilities

The college has a responsibility to ensure that information security is properly managed.

All Managers, Heads and Directors are responsible for ensuring compliance with this policy.

Key management responsibilities include:

- Compliance with data protection policies and regulations;
- Ensuring members of staff are instructed in their security responsibilities;

7.1 Head of Information Systems and Digital Infrastructure

- the development and upkeep of this policy
- ensuring this policy is implemented and supported by appropriate documentation, such as procedures
- ensuring that documentation is relevant and kept up-to-date
- ensuring this policy and subsequent updates are communicated to all staff

Equality Impact Assessment

Before carrying out an EIA, you should familiarise yourself with the College's EIA Policy Statement and Guidance, along with further information and resources which are available on Sharepoint

EIA covers **strategies**, **policies, procedures, plans, provisions, criteria, functions, practices and activities, including decisions and the delivery of services**, but will be referred to hereinafter as 'policy/practice'.

Policy/Practice (name or brief description):	**IT Security Policy**
Strategy/Policy includes Equalities Statement of Inclusiveness? Yes	**Text to be included in strategy/policy:** **Statement of Inclusiveness** West Lothian College is an inclusive organisation and all policies, procedures, strategies, plans, provisions, criteria, functions, practices and activities, including decisions and the delivery of services are assessed to consider the impact on staff and students covered by the Equalities Act 2010 by the completion of an Equalities Impact Assessment (EIA). Protected characteristics are defined as age, disability, gender reassignment, marriage or civil partnership (in employment only), pregnancy and maternity, race, religion or belief, sex, sexual orientation.
Reason for Equality Impact Asessment (choose from the following options):	
• Proposed new policy/practice • Proposed change to an existing policy/practice • Undertaking a review of an existing policy/practice • Other (please give detail):	Proposed change to an existing policy/practice.

Person responsible for the policy area or practice:	
Name: Job title:	Simon Earp Vice Principal, Performance and Improvement
An Equality Impact Assessment must be carried out if the policy/practice: • affects **operational** or **strategic functions** of the college • is relevant to the promotion of equality (in terms of the Public Sector Equality Duty 'needs' as set out in the Policy and Guidance)	
Why the EIA is being carried out	Affects operational and strategic functions of the college.
Equality Groups Relevant to the Policy/Practice, identify which of the undernoted equality groups are impacted upon:	
• Age • Disability • race (including ethnicity and nationality) • religion or belief • sex • sexual orientation • gender reassignment • pregnancy and maternity • marriage or civil partnership	None.

Record your assessment against the following statements:

Statement	**Equality assessment**
Detail the evidence of the needs of the identified equality groups and any gaps in information	Not applicable.
Will application of this policy/practice lead to discrimination (direct or indirect),	No

harassment, victimisation, less favourable treatment for particular equality groups?	
If yes, how will the policy/practice be changed to contribute to advancing equality of opportunity	
State how this policy/practice will foster good relations:	The policy sets of rules, policies and procedures designed to ensure all end users and networks within the organisation meet minimum IT security and data protection security requirements
Will the policy/practice create any barriers for any other groups?	No
If yes, how will the policy/practice be changed to contribute to advancing equality of opportunity	
Which equality groups or communities have been consulted in the development and review of this policy/practice?	Representatives from the college cyber and information security groups

Equality Impact Assessment Outcome Select one of the four options below to indicate how the development/review of the policy/practice will be progressed and state the rationale for the decision. (Delete the options that do not apply):	
Option 1: No change required – the assessment is that the policy/practice is/will be robust.	Minor changes in terms of key owners/stakeholders identified in the execution of the Policy/Procedure.
Monitoring	
When will the policy/practice next be reviewed?	December 2025
Publication of EIA	
Can this EIA be published in full, now? Please state Yes or No	Yes

If No – please specify when it may be published or indicate restrictions that apply:	
Sign-off	
EIA undertaken by Name: Bill Dunsmuir, Head of Information Systems and Digital Infrastructure Date: 17 January 2023 Accepted by person responsible for the policy/practice named above: Name: Simon Earp - Vice Principal, Performance and Improvement Date: 30 January 2023 Approved by Equalities Committee Date:	

Retain a copy of this form for your own records and attach a copy to the bottom of the document to which it refers. Send to lbyrne@west-lothian.ac.uk for review and publication.