IT Security Policy

Authors: Paula White, Facilities Manager

Impact Assessment Date: November 2015

Dat**e:** October 2015

Reviewed Brian Smillie March 2018

Equality Impact Assessment/ March 2018/Review Date March 2020

Contents

1 Introduction.. 1

2 Systems and Data Collection.. 1

3 Key Principles 1

4 Confidentiality 2

5 Responsibilities 2

6 Availability/Inventory 8

1 Introduction

West Lothian College is committed to protecting its computer systems, personal data, College information systems and the online safety of staff and students. This IT Security Policy should be read in conjunction with other IT Policies by staff and students to raise awareness their responsibilities in respect of IT Estate.

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. Personal devices which are used for College business, and therefore hold College data must be password protected.

2 Systems and Data Collection

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 – Sun Systems
- Human Resources and Systems
- Moodle VLE (virtual learning environment)
- Unit E (including student attendance)
- FIMS (student logins)
- Tabs FM (Intranet services).
- Website services including online course, job and student funding applications.
- E-mail System.
- Hunter (Contracts database)
- Windows Active Directory
- Serengeti
- Janet Network

3 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 following 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
GDPR 2018

4 Confidentiality

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. Any storage devices such as home PCs, USB and external hard drives must be scanned with the College anti-virus software. Users should also be familiar with the College’s Bring Your Own Device Guidelines.

5 Responsibilities

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

Staff Responsibilities

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

- IT Staff Acceptable Use Policy
- Data Protection Policy
- Freedom of Information Model Publication Scheme
- Social Media Policy
- Bring Your Own Device Guidelines

- IT Password Guidelines
- Child Safeguarding Policy
- Protecting Vulnerable Groups Policy Procedure (students)

Student Responsibilities

- IT Student Acceptable Use Policy
- Data Protection Policy
- Freedom of Information Model Publication Scheme
- Social Media Policy
- Bring Your Own Device Guidelines
- IT Password Guidelines

All of the above documentation can be found on Serengeti.

All users must adhere to this policy, and report any security breaches or incidents to the Facilities Management (FM) team straight away.

Management Responsibilities

The College has a responsibility to ensure that information security is properly managed. The FM Management team is responsible for:

- 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 relevant staff
- ensuring that serious breach notification is investigate and the appropriate action taken.

The Assistant Principal in Curriculum Support and Finance
is responsible for providing up-to-date information on data protection matters.

The Head of Quality and Learner Services is responsible for ensuring secure transmission of student records data to partner organisations. The Assistant Principal in Curriculum and Planning is responsible for providing up-to-date information on safeguarding requirements and current issues relating to on-line safety.

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

Sharing Data and Data Transfer

The College works with partner organisations (such as SFC, 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 Head of Quality and Learner Services and the Assistant Principal Curriculum and Planning.

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 and after completion of the Computer Access Files form.

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, HR will ask the employee to 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.
- 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.
- Any change to roles should be reflected in access or denied access to suit the new role. This should be communicated through HR.

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 IT 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 appropriate Manager.

Integrity

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/Anti Encryption 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 IT Services immediately. Similarly, if a member of staff is unsure whether the installed virus protection software is being automatically updated he/she must contact IT Services immediately.

Users should report any viruses detected/suspected on their equipment immediately by calling the Facilities Helpdesk.

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.

Logging onto multiple devices to allow others to download software is strictly forbidden and users doing so will be in breach of College procedures and maybe investigated and subject to College Disciplinary Procedures.

Key Information and Business Systems

Key systems shall be protected by physical security and user access control measures and data storage and backup. Access to key IT systems and key data and information will only be granted on a need to know basis
All hard copy staff, student, financial 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.

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 and limited to IT Services only.

PCs or terminals should be secured by password access control when not in use. Failure to protect the Network may result in Disciplinary action being taken.

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.

Key IT systems shall be protected by UPS.

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.

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 IT Helpdesk.

Network Security

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

It is the responsibility of the FM Deputy 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.

Software installation by any personnel other that IT Services is not permitted. Requests for installs should be generated through the Tabs FM database. The FM Deputy 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.

Hardware and Software Acquisition

All hardware and software must be discussed and approved by the FM Deputy Manager prior to raising PECOS orders. Any orders raised will be passed for authorisation from the FM Deputy Manager.

Software installation by any personnel other than IT Services is not permitted.

All hardware will be installed onto College systems by IT Services staff only.
The placement, re-positioning and removal of computer equipment can only be authorised by, and carried out under instruction from the FM Deputy Manager**.**

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:

- Induction sessions
- Moodle
- Lecturer input
- Student Association

Incident Management

Users must contact the IT Services 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 IT network at risk will be disconnected.

6 Availability/Inventory

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 on a PC hard drive. 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 and recovery time in the event of an emergency and should be regularly tested.

Equipment Inventory

An inventory of all computer equipment and software will be maintained. The Facilities staff has responsibility for the inventories on all of the College sites.

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 Facilities staff for all College installed software applications.

west lothian college

EQUALITY IMPACT ASSESSMENT

IT Security Policy

Author: P White

Date: March 2018

Review date: March 2020

What is an equality impact assessment?

An equality impact assessment (EIA) is a tool that helps West Lothian College (WLC) make sure our policies, and the ways we carry out our functions, do what they are intended to do for everybody. This process can help the college to deliver excellent services by making sure that the diverse needs of students and staff are considered.

By carrying out EIAs, WLC will also ensure that the services we provide fulfil the requirements of equality legislation.

Further web based information resources on the range of issues considered as part of and EIA, as well as background and procedural information, can be found at Annex A.

What is the purpose of an EIA?

EIAs offer an opportunity for WLC staff to think about the impact of our work on students and other members of staff. EIAs should make sure that equality is placed at the centre of policy development and review, service delivery and decision making. EIAs should be used to take action that will promote equality for all.

The EIA process focuses on:

- initial screening;
- scoping and defining;
- information gathering;
- making a judgement;
- action planning; and
- publication and review.

EIAs can be used to:

- increase participation with students and staff in policy, procedural and project development;
- change the culture of public decision making by encouraging more transparency; and
- proactively promote equality and put it at the centre of college decision making.

How are EIAs carried out?

The EIA process should be used when developing or reviewing:

- policy
- strategy
- procedure
- function
- decision making
- project
- reviews
- services
- organisational change

At the end of the process there will be a summary report published to let people know the outcome of the assessment. The actual process is described fully below in section 2.

When are EIAs carried out?

In line with statutory requirements, WLC must conduct impact assessments as soon as new policies, practices, decisions etc are considered. It should be an integral part of the development process. Existing policies and procedures should have EIAs conducted on them as part of the rolling policy review process.

Who carries them out?

The responsibility for conducting EIAs lies at the service level. Appropriate managers are responsible for conducting EIAs, when necessary. Frontline staff are important in the assessment process as they will be involved in implementing actions and changes that the assessment identifies as being necessary. Equalities officers have an important role to ensure that their colleagues are properly trained in how to carry out EIAs, supporting staff to improve EIAs where needed, monitoring the quality of EIAs being produced

and signing off those which are sufficiently rigorous. When considering the equalities implications it is necessary to involve others who may offer challenge to views or some evidence of impact.

Why do we carry them out?

The EIA process is legal requirement and good practice, it should be seen as a means to help WLC to improve its policies, strategies, procedures, projects etc. EIAs also have an important part to play in helping guide an institution through organisational change and development. They should be conducted in such a way as to benefit the whole of the WLC community, and not just certain groups.

In practice this means meeting the general duty in relation to students and staff as follows:

- to eliminate discrimination, harassment, victimisation and any other conduct that is prohibited by law;
- to advance equality of opportunity;
- to foster good relations between persons who share a relevant protected characteristic and persons who do not share it.

Who are the target equality groups?

The EIA focus's on certain target groups. These groups are known to experience more disadvantage than others. For instance they may be more likely to be adversely affected by, or omitted from the benefits of, a policy or service.

The groups cover certain 'protected characteristics'' set out in the Equality Act 2010. The EIA focuses on these protected characteristics to try to find out whether or not people who share them are benefiting from a strategy, policy, service, project, decision etc.

The protected characteristics (last updated 9 June 2014) are:

- age
- disability
- gender reassignment
- marriage and civil partnership (not a protected characteristic for Further and Higher education)
- pregnancy and maternity
- race
- religion or belief
- sex
- sexual orientation

These groups are not homogeneous and people within these groups have different and individual needs. Many will be members of several of the targeted groups. Their experience of unlawful discrimination can involve a variety of factors which should be considered as part of the EIA process.

Section 2: The Equality Impact Assessment Process

Phase 1: Screening and Prioritisation

The first phase of the Equality Impact Assessment (EIA) is to screen the policy, practice, strategy etc to establish if it has an impact upon anyone because of a protected characteristic (age, disability, ethnicity, gender, gender reassignment, pregnancy and maternity, race, religion or belief, sexual orientation).

A single EIA should be conducted and recorded for each individual policy, practice, strategy etc.

Please compete the following:

Name of policy/ practice/strategy/ decision	**Named individual responsible for policy/practice/strategy/ decision**	**Name of person conducting initial EIA**
IT Security Policy	**Paula White**	**Paula White**

Supporting notes to help in the completion of Phase 1

- Consider impact in terms of the protected characteristics and other groups who may experience disparities in opportunity.

- Make use of existing knowledge, experience, research and consultation.

- Caution is needed not to consider a policy or practice ‘equality neutral’ just because no evidence of adverse impact exists (e.g. you might find little research exists with regard to equality areas such as sexual orientation).

- When thinking about positive impact consider ways to tackle discrimination, promote equality of opportunity and promote good community relations.

Q1. Given the aims of the proposed policy, practice, strategy decision is it likely that there will be a negative impact on one or more of the groups named above. Or is it clear at this stage that it will be equality neutral?

Protected Characteristic	**Impact (explain)**
Age	None
Disability	None
Gender reassignment	None
Pregnancy and maternity	None
Race	None
Religion or belief	None
Sex	None
Sexual orientation	None

Comments:

This policy will have a positive impact on the above groups as its main aim is to ensure security of the individual and the college systems.

No negative impact is anticipated for any of the above groups. This policy is committed to protecting the college computer systems, personal data, college information systems and the online safety of staff and students.

Q2. For which groups are there likely to be a negative impact? What is this impact likely to be, and what plans could be built in to address negative impacts and to add measures which promote a positive impact at this stage?

Protected Characteristic	Impact (explain)
Age	N/A
Disability	N/A
Gender reassignment	N/A
Pregnancy and maternity	N/A
Race	N/A
Religion or belief	N/A
Sex	N/A
Sexual orientation	N/A

Comments:

This policy will not have a negative impact on any of the above groups, therefore no further action is required.

Q3. At this stage, how could the policy, project or strategy promote positive impacts for any of the groups named above?

The policy ensures all users take appropriate precautions to ensure that another user cannot gain unauthorised access using their equipment and that no computer or mobile device is effecting the integrity of the College's IT network. Any known security breach should be report to the college.

Q4. Is a full impact assessment required? YES / NO (use box to explain rationale behind decision)

No further assessment required as there is no discerned negative impact on any of the protected characteristics groups. The IT Security Policy exists to strengthen the security of all users impartially.

Signature of named individual responsible for policy	**Signature of individual responsible for carrying out initial impact assessment (if different from previous)**	**Date of completion of initial impact assessment**
P White	**P White**	**26/3/18**

In the event of a full impact assessment being required this document must be attached and used as part of that process