# E-Mail and Computer Network Responsible Use Policy

Author: Head of Information Systems and Digital Infrastructure

Date: September 2024

Review Date: September 2026

Revised Equality Impact Assessment Date: September 2024

**History of Changes**

| Version | Description of Change | Authorised by | Date |
|---|---|---|---|
| 1.0 | New Policy | B Dunsmuir | 05/09/2024 |

## 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.

We also acknowledge our responsibilities under The Human Rights Act 1998 to protect and promote fundamental human rights and freedoms, such as the right to life, personal liberty, an education, freedom of expression and the prohibition of torture.

Please see end of this document for EIA.

# 1 Introduction

West Lothian College provides Internet access and other computer services to staff and students for communication and other purposes, to support education and to enhance the learning process. The purpose of this policy is to outline the acceptable and unacceptable use of the college's IT Estate. This includes responsible and legal use of the technologies and facilities made available to staff, students and associates of the college.

In the policy detail below, the term 'network resources' refers to all network activity, including file storage, email and "Internet access" (defined as use of Web browsing and Social Networking applications such as Facebook and Twitter).

College network resources are provided to facilitate a person's activities as an employee, student of the college or registered user with West Lothian Council's Library Service, specifically for learning and teaching, training, administrative or research purposes.

This policy is intended to provide a framework for such use of all college IT resources. It should be interpreted such that it has the widest application and applies to all computing, telecommunication, and networking facilities provided by any department or section of the college.

# 2 Policy

By using the email and network facilities and services, you agree to adhere to this policy.

## 2.1 Malware and Viruses

- 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.
- These programmes can allow people unauthorised access to the college's systems.
- The integrity of the college computer systems is jeopardised if users do not take adequate precautions against malicious software, such as computer virus programs and malicious content (malware) including but not limited to email, websites, and shared files.
- Everyone must use care when transferring data between their personal devices, computers and phones, and the college network.
- Users should report any college equipment they suspect are not protected by anti-virus or if the anti-virus is out of date by logging a call via the Helpdesk.
- Users should report any viruses detected/suspected on college equipment immediately by logging a call via the Helpdesk.

## 2.2 Authorised use of Services and User Accounts

- Staff, students and contractors should only access systems for which they are authorised.
- All individually allocated usernames and passwords are for the exclusive use of the individual to whom they are allocated. The user is personally responsible and accountable for all activities carried out under their username.
- The password associated with a particular personal username must not be divulged to another person. Attempts to access or use any username, which is not authorised to the user, are prohibited.
- No-one may use, or attempt to use, computing resources allocated to another person, except when justifiably authorised by the provider of those resources.
- 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.
- All users must take appropriate precautions to ensure that another user cannot gain unauthorised access using their equipment
- Computing devices should be secured with password access control when unattended
- 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.
- Examples of unacceptable behaviour:

    - Allowing others to access college network resources which they do not have permissions for or allowing others to download software under your login.
    - frivolous use of college owned computer laboratories, especially where such activities interfere with others' legitimate use of IT services;
    - non-academic activities which generate heavy network traffic, especially those which interfere with others' legitimate use of IT services or which incur financial costs;
    - unreasonable use of college hardware, software, peripherals, media or consumables for personal purposes especially when such use incurs financial costs;
    - Users may not, under any circumstances, monitor, intercept or browse other users' e-mail messages or Internet activity unless authorised to do so.

## 2.3 Maintaining Resource Integrity

- No person shall jeopardise the integrity, performance or reliability of computer equipment, network equipment, software, data and other stored information.
- Reasonable care should also be taken to ensure that resource use does not result in a denial of service to others.

- Examples of unacceptable behaviour:

    - Unauthorised installation of software on any college computing device.
    - Unauthorised hacking and computer misuse
    - knowingly accessing or forwarding malicious, or harmful emails or content which may cause Infection, encryption or loss or damage to data.
    - Interfering or attempting to interfere in any way with information belonging to or material prepared by another user.
    - Making unauthorised copies of information belonging to another user.

## 2.4 Misuse of College Resources

Inappropriate use of network resources is forbidden, for example, activity involving:

- unsolicited advertising, often referred to as “spamming”;
- sending of unwanted e-mail (usually advertisements) or images and chain letters.
- the use of departmental academic mailing lists for non-academic purposes;
- unauthorised resale of college or JANET services or information.
- unauthorised commercial activity i.e. for personal financial gain, advertising or political activity.

## 2.5 Misrepresenting yourself

- You will not attempt to mislead others as to your identity, either by providing false information when subscribing to, or posting to, individuals or discussion groups, or by forging the headers and addresses in an email message.
- Alteration of the source of electronic mail, message or posting is unethical and could have legal implications.

## 2.6 Harassment

- Distributing material that is offensive, obscene or abusive, may be illegal and may also contravene college codes on harassment.
- Flaming is not permitted in any communication. A flame is when you call someone names, are overtly rude, or are blatantly sarcastic or condescending.
- All communication must be stated in polite terms. In discussion groups, a large audience will see your messages, so be careful what you write.

- Good interpersonal etiquette should be observed at all times, even online and in emails. These include, but are not restricted, to the following:

    - Be polite
    - Use appropriate language; do not swear or use vulgar language
    - Do not reveal the personal email address, home address or telephone of any person.

- Users of college computer systems must make themselves familiar with, and comply with, the college policies concerning all forms of harassment.

## 2.7 Contact with extremist groups

- The Government has defined extremism in the Prevent guidance as: “vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs. We also include in our definition of extremism calls for the death of members of our armed forces”.
- Any academic staff or students who need to undertake research in relation to these groups should discuss this with their Line Manager in the first instance.
- Approval for this research, once approved, should be requested to the Digital Infrastructure team, who can adjust security settings, upon receipt of a Helpdesk ticket, as these will normally block access to extremist group websites.
- Any non-authorised contact with extremist groups may have to be reported to the Police, in keeping with Prevent guidance.

## 2.8 Copyrighted Material

All users must adhere to the college’s Copyright Policy.

Examples of unacceptable behaviour:

- intellectual property rights infringement, including copyright, trademark, trade secret, patent, design and moral rights;
- the distribution or storage by any means of pirated software or copyright music and video;
- the use of CDs, disks or other media for the purpose of copying unlicensed copyright software; or
- the use of other people’s web site material without the express permission of the copyright holder.

## 2.9 Social Media

- All users must adhere to the college’s Social Media Policy.

### 2.10 Data Protection

- All users should comply with current legislation on data protection (e.g., Data Protection Act, GDPR) and be familiar with college Policies regarding personal data protection.

## 3 Staff AUP

- Staff must not leave computers unattended which are logged on to college systems. If leaving a workstation whilst logged in the device should be locked and password protected.
- No department has the authority to purchase hardware or software without first discussing this with the Digital Infrastructure (DI) Manager or other members of that team. All orders raised on Pecos of this nature will be passed to DI for authorisation.
- To conserve disk space on the server, users should archive and delete email and old files on a regular basis. Attachments should be detached and stored in a personal storage area until used then deleted. This could include local storage such as memory sticks as well as centralised storage on the servers.

### 3.1 Personal Use

Incidental and occasional personal use of e-mail and Internet access is permitted so long as such use a) does not disrupt or distract the individual from the conduct of college business (e.g. due to volume, frequency or time expended) or restrict the use of those systems to other legitimate users and b) complies with this policy.

- College computing and telephony resources are provided to facilitate a person's work as an employee of the college, specifically for educational, training, administrative or research purposes.
- Use for other purposes, such as personal electronic mail or recreational use of the World Wide Web, is a withdrawable privilege not a right. Any such use, or any other form of personal use must not interfere with the user's duties or studies or any other person's use of computer systems and must not, in any way, bring the college into disrepute.
- Commercial work for outside bodies, using centrally managed services is not permitted.
- The college recognises that there are occasions when a user may wish to use both the email system and the Internet for personal purposes. Such usage should be kept to a minimum and conducted during meal times or other breaks or outside working hours. In making any personal use of the facilities the user must adhere to the terms of this agreement.
- If it is considered by the college that excessive, inappropriate or wasteful use is being made of any of the college Computer Network for personal use, action may be taken against users.

- Users must not cause network congestion by duplication of frivolous material, or by unnecessarily copying emails to people who will have little interest in their contents.

### 3.2 Privacy

Staff privacy is seen by the college as a privilege and not a right. However, access to staff files will not normally be given to another member of staff unless authorised by an appropriate Senior Manager. The college reserves the right to access the mailbox / computer files of employees during a period of their absence.

## 4 Monitoring of Email and Internet Activity

Systems Administrators have access to email, Internet usage information and files stored on the network as part of their network monitoring rights and the college reserves the right to monitor email content and traffic (including Internet access) across the network.

- The college reserves the right to use appropriate hardware and software monitoring tools to ensure compliance with the terms of this and all other related IT procedures and policies.
- The college reserves the right to access and disclose the contents of a user's e-mail messages, in accordance with its legal and audit obligations, and for legitimate operational purposes. Encryption keys must not be used without prior agreement with system administrators.
- Network systems record email usage and Internet access and activity. Unless authorised by the Digital Infrastructure Manager, Systems Administrators will not monitor the content of email messages or disclose any of the logged or otherwise collected information.
- Network and computer operations personnel, or system administrators, may not monitor other users' e-mail messages other than to the extent that this may occur in the normal course of their work.

### 4.1 File Scanning

- The college reserves the right to scan college resources for storage of illegal or inappropriate material.
- If such material is found on college resources the college reserves the right to immediately and without notification, delete the data and may suspend the user account, subject to further investigation under breach of this agreement.
- Email and Internet filtering technologies are used to ensure a safe and secure network.
- Download of certain file types is restricted to maintain security. These technologies are automated and, as a consequence, may prevent email delivery or access to specific web sites that are, in fact, appropriate. If this is suspected then network should log a call via the college Helpdesk, to draw attention to a website’s validity –

staff will receive an automated message if an email is blocked on the basis of banned file attachments.

## 5 Compliance

It is the responsibility of each individual to ensure they comply with this policy. If you are in doubt as to the legitimacy of a given course of action please discuss this with your Line Manager.

This policy is not exhaustive and inevitably new social and technical developments will lead to further uses which are not fully covered. Where there is any doubt, staff should initially contact their line manager. Further advice should be sought from the IT Services, whose staff will ensure that questions are dealt with at the appropriate level within the college.

### 5.1 Reporting Breaches

- Any suspected breach of this procedure should be reported to a member of the IT Services or the Digital Infrastructure Manager. The responsible senior member will then take appropriate action within the college disciplinary policy, in conjunction with other relevant sections of the college.
- IT Services staff will also act when infringements are detected in the course of their normal duties.

### 5.2 Disciplinary or Corrective Action

- The college reserves the right to audit and / or suspend without notice any account pending an enquiry.
- Users may also be subject to limitations on their use of college resources.
- Users who breach this agreement may have their access to Internet facilities suspended while an investigation takes place and may be open to disciplinary or legal action initiated by the college or a third party.

# Equality Impact Assessment

| | |
|---|---|
| **Policy/Practice (name or brief description):** | E-mail and Computer Network Responsible Use Policy |
| **Strategy/Policy includes Equalities Statement of Inclusiveness?** | **Yes**<br><br>**Statement of Inclusiveness**<br><br>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).<br><br>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.<br><br>We also acknowledge our responsibilities under The Human Rights Act 1998 to protect and promote fundamental human rights and freedoms, such as the right to life, personal liberty, an education, freedom of expression, and the prohibition of torture. |
| **Reason for Equality Impact Assessment (choose from the following options):** | |
| • Proposed new policy/practice<br>• Proposed change to an existing policy/practice<br>• Undertaking a review of an existing policy/practice<br>• Other (please give detail): | New consolidated Policy which now includes staff, students and other users. |
| **Person responsible for the policy area or practice:** | |
| Name:<br><br>Job title: | Bill Dunsmuir<br><br>Head of Information Systems and Digital Infrastructure |

| **An Equality Impact Assessment must be carried out if the policy/practice:**<br>• affects **operational** or **strategic functions** of the college<br>• 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 functions of the college<br>• is relevant to the promotion of equality (in terms of the Public Sector Equality Duty 'needs' as set out in the Policy and Guidance) |
| **Equality Groups**<br>Relevant to the Policy/Practice, identify which of the undernoted equality groups are impacted upon: | |
| • Age<br>• Disability<br>• Race (including ethnicity and nationality)<br>• Religion or belief<br>• Sex<br>• Sexual orientation<br>• Gender reassignment<br>• Pregnancy and maternity | There is some evidence that extremism and internet misuse may be more likely to occur in some protected groups including those with disabilities (neurodiversity and mental health), sex (male), race and religion or belief without stating a causal effect, e.g. A Systematic Review of Neurodivergence, Vulnerability, and Risk in the Context of Violent Extremism (crestresearch.ac.uk). |

## Record your assessment against the following statements:

| **Statement** | **Equality assessment** |
|---|---|
| Which equality groups or communities have been consulted in the development and review of this policy/practice? | None on this occasion. |
| Detail the evidence of the needs of the identified equality groups and any gaps in information | As above, breaches of the policy will be by staff and students who are in various protected groups. The policy promotes a fair and equitable approach to dealing with breaches which is in line with UK legislation. |
| Will application of this policy/practice lead to discrimination (direct or indirect), harassment, victimisation, less favourable treatment for particular equality groups? | It should not, but proactive risk assessment should continue to be used for staff and students who are known to have breached the law in this area to ensure that individualised and equitable treatment is in place. |

| | |
|---|---|
| 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 makes it clear the expectations of behaviour of staff, students and other stakeholders with the view that everyone is kept safe. |
| Will the policy/practice create any barriers for any other groups? | No |
| Considering The Human Rights Act 1998, does this policy/practice impact upon any of the following rights:<br>The right to life<br>The right not to be tortured or treated in an inhuman way<br>The right to protection of property<br>The right to education<br>The right to private and family life<br>The right to personal liberty and security<br>The right to a fair trial<br>The right to freedom of religion and belief<br>The right to freedom of expression<br>The right to non-discrimination in connection with human rights | No |
| If yes, how will the policy/practice be changed to contribute to advancing equality of opportunity | N/A |

**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. | Option 1 is selected.<br><br>Recommend review of policy breaches against equality characteristics to monitor validity of this decision. |

| | |
|---|---|
| **Monitoring** | |
| When will the policy/practice next be reviewed? | September 2026 |
| **Publication of EIA** | |
| Can this EIA be published in full, now? Please state Yes or No<br><br>If No – please specify when it may be published or indicate restrictions that apply: | Yes |
| **Sign-off** | |
| EIA undertaken by<br><br>Name:<br><br>Date:<br><br><br>Accepted by person responsible for the policy/practice named above:<br><br>Name:<br><br>Date:<br><br><br>Approved by Equalities Committee (by exception)<br><br>Date: | Beth Brownlee<br><br>06.09.2024 |

Once completed, updated documents should be agreed with the Executive Leadership Team then uploaded to the college website and Sharepoint. The approved copy is then the source document.