

Business Owner:	Organisation Support & Development
Document Title:	Email Policy LWETB
Document No.	ICT016/EM/V4/24
Version No.	ETBI 22
Approved By:	Chief Executive LWETB
Noted by:	LWETB Board
Date Noted:	November 2024

LONGFORD AND WESTMEATH EDUCATION And TRAINING BOARD

EMAIL POLICY

TABLE OF CONTENTS

1. Purpose	3
2. Scope.....	3
3. User Responsibilities.....	3
3.1 Acceptable Uses.....	3
3.2 Unacceptable Uses	4
4. Privacy Guidelines	5
5. Security	6
6. Operational Guidelines.....	6
7. Compliance	7
8. Policy Review and Continuous Improvement.....	7
9. Ownership and Approval.....	7

1. Purpose

The purpose of this policy is to ensure the proper use of e-mail by Longford Westmeath Education and Training Board (LWETB) Users”. Usage of LWETB e-mail resources is a privilege that is extended to, but not limited to employees (both full and part time), students, apprentices & learner’s contractors, interns, partners and / or consultants, external individuals, and organisations, to be referred to as “Users”. E-mail users must follow the same code of conduct expected in any other form of written or face-to-face business communication and have a responsibility to use email in an efficient, effective, ethical, and lawful manner.

LWETB may supplement or modify this policy for users in certain roles. This policy for Email Usage complements similar LWETB policies, such as the Technology Acceptable Usage Policy. A comprehensive list of ICT policies may be located in the ICT Policy Framework.

2. Scope

This policy applies to all “users” of LWETB provided email systems either owned or managed by LWETB Individuals covered by the policy include (but are not limited to) employees (both full and part time), contractors, interns, partners and / or consultants, external individuals and organisations, utilising email facilities provided by LWETB.

This policy applies to any corporate e-mail system that LWETB has or may install in the future. It also applies to employee use of personal e-mail accounts via browsers, whilst using LWETB ICT resources as directed below.

3. User Responsibilities

LWETB supports the installation and usage only of approved e-mail clients.

Username will be assigned by LWETB and will reflect internally mandated e-mail naming conventions.

3.1 Acceptable Uses

The following is a broad and non-exhaustive list of examples of acceptable usage of LWETB email resources.

- Communicating in a professional manner with other LWETB users about work-related matters.
- Communicating in a professional manner with third parties on behalf of LWETB for business purposes.
- Personal communications that are brief and do not interfere with work responsibilities.

3.2 Unacceptable Uses

The following is a non-exhaustive list of actions or activities that would generally constitute unacceptable use. (**Note:** This list is solely intended to be a guideline for users when considering what is unacceptable use and is not comprehensive.)

- Creating and exchanging messages that could be interpreted as offensive, harassing, obscene, racist, sexist, ageist, pornographic or threatening.
- Creating and exchanging information that is in violation of copyright or any other law. LWETB is not responsible for user(s) usage of e-mail that breaks laws.
- Personal communication that interferes with work responsibilities.
- Opening file attachments from an unknown or untrustworthy source, or with a suspicious or unexpected subject line. Should any clarification be required, notify LWETB immediately via corporate@lwetb.ie if a suspicious email / attachment is received.
- Sending confidential information to unauthorised persons or violating LWETB Data Protection Policies. Otherwise using e-mail in a way that increases LWETB legal and regulatory liability.
- Communications that strain the LWETB IT network or other systems unduly, such as sending large files to large distribution lists.
- Communications to distribution lists of only marginal interest to members and replying to the entire distribution list when a personal reply is as effective.
- Communications with non-specific subject lines, inarticulate language, and without clear purpose.
- Forwarding work-related e-mail messages to personal accounts, because of unacceptable risks associated with privacy, security, and compliance. This does not include your personal pension, salary, or HR information.
- Using an LWETB email address for any internet subscription, unless there is an underlying organisational rationale. Should further clarification be required, contact your line manager
- Forwarding information to mobile devices without the explicit permission of LWETB
- Using any e-mail system, other than the corporate e-mail system, for LWETB related communications.
- Circulating chain letters and/or commercial offerings.
- Promoting or publishing an employee's political or religious views, operating a business or for any undertaking that offers personal gain or benefit.

As a user of LWETB email resources, you are expected to uphold all Irish legislation and relevant legislation of the European Community. All users of LWETB email resources should ensure that they are fully aware of and understand any of the relevant legislation, which applies to the sending of electronic communications. A comprehensive list of ICT policies may be located in the ICT Policy Framework.

4. Privacy Guidelines

LWETB maintains ownership of all LWETB emails which includes the right to monitor and review work e-mail activity to ensure compliance with this policy, as well as to fulfil LWETB responsibilities under relevant laws and regulations of both Ireland and the E.U., for example, GDPR. **Users should have no expectation of privacy** to their use of corporate / work emails.

- On resignation, termination or departure from LWETB, LWETB will immediately deny access to e-mail, including the ability to download, forward, print or retrieve any message stored in the system, regardless of sender or recipient.
- Anyone who ceases to become a user of LWETB email resources, will have their access disabled on leaving date and mailboxes archived within one (1) month of their leaving date. The employee's line manager may request that access be given to another user who may remove and utilise any needed information within the same time frame. Mailboxes will subsequently be deleted in line with LWETB data retention policy / LWETB contractual obligations.
- LWETB reserves the right to intercept, monitor, review and/or disclose any and all messages composed, sent, or received on the corporate e-mail system. Intercepting, monitoring and reviewing of messages may be performed with the assistance of content filtering software, or by designated LWETB employees and/or designated external entities.

The ICT Policy Framework provides further detail on the type of monitoring that is possible to undertake. Should further clarity be required, contact Head of Corporate Services.

- LWETB reserves the right to alter, modify, re-route, or block the delivery of messages as appropriate. This includes but is not limited to:
 - Rejecting, quarantining, or removing attachments and/or malicious code from messages that may pose a threat to LWETB resources.
 - Discarding attachments, such as music, that are considered to be of little business value and involve a significant resource cost.
 - Rejecting or quarantining messages with suspicious content.
 - Rejecting or quarantining messages containing offensive language or topics.
 - Re-routing messages with suspicious content to designated LWETB employees for manual review.
 - Electronic messages, including draft documents saved to or on LWETB I.C.T. resources are potentially legally discoverable and admissible as evidence in a court of law.
 - Any content created with the e-mail system is considered the intellectual property of LWETB.

Any evidence of suspected or alleged illegal activity discovered during monitoring or reviews will be dealt with through LWETB disciplinary procedure and may lead to a further criminal investigation. See the “Compliance” section of this policy for further information.

5. Security

As with any other type of software that runs over a network, e-mail users have the responsibility to follow sound security practices.

- E-mail users should not use e-mail services to transfer sensitive data, such as usernames, passwords, PPS numbers and account numbers over the Internet. Users should not use the e-mail system to transfer sensitive data, except in accordance with LWETB GDPR / Data Protection Policies. Sensitive data passed via e-mail over the Internet could be read by parties other than the intended recipients, particularly if it is clear text. Malicious third parties could potentially intercept and manipulate e-mail traffic.
- In an effort to combat propagation of e-mail viruses, certain attachment types may be stripped at the corporate e-mail gateway. Should this create a business hardship, users should contact LWETB for further information.
- Attachments can contain viruses and other malware. User should only open attachments from known and trusted correspondents. LWETB Corporate Services or ICT Support Services should be notified immediately if a suspicious email / attachment is received.
- Spam communications are automatically filtered. Errors, whereby legitimate e-mail can be filtered as spam, while rare, can occur. If business-related mail messages are not delivered, users should check their local spam folder. If the message is not there, users should call LWETB.

Due to the polymorphic nature of Spam communications, occasionally some of these spam communications may reach users email folders. In these incidents, a user(s) should notify LWETB Corporate Services immediately.

- Users should always be vigilant when clicking on weblinks embedded in an email, especially if any personal / sensitive data such as usernames or passwords are sought. Even if the sender is known to you, if you are suspicious about the information sought, either contact the relevant person by phone or forward the email to LWETB for further information. Such approaches may be a phishing attack and these attacks tend to be carried out for the purposes of unlawful exploitation.

6. Operational Guidelines

LWETB employs certain practices and procedures in order to maintain the security and efficiency of electronic messaging resources, to achieve LWETB objectives. These practices and procedures are subject to change, as appropriate or required under the circumstances.

- For ongoing operations, audits, legal actions, or any other known purpose, LWETB saves a copy of every e-mail message and attachment(s) to a secure location, where it can be protected and stored for seven (7) year period. Recovery of messages from this archived store is prohibited unless requested by the data owner or required for legal reasons.
- To deliver mail in a timely and efficient manner, message size must be less than 150 MB. Messages larger than 150 MB will be automatically blocked, and users will be notified of non-delivery. Should this create a business hardship, users should contact LWETB.

- All written communication constructed using LWETB email resources should meet the highest level of professionalism, courtesy, and respect. Electronic communication is frequently inadequate in conveying mood and context; therefore, the user should carefully consider how the recipient may interpret a message before sending any message.

7. Compliance


Individuals found to be in breach of this Email Policy, may be subject to disciplinary action, up to and including dismissal. Should an investigation regarding compliance with this policy determine that there may be a case to answer by an Employee / User, the matter will be referred into the appropriate stage of the relevant disciplinary procedure as appropriate to that Employee / User.

For the avoidance of doubt, where questions remain as to what constitutes “appropriate use”, contact LWETB for full clarification.

8. Policy Review and Continuous Improvement

This document is subject to review every two (2) years by the Senior Leadership Team in line with best practice, in light of changes in legislation and guidance from sources such as Internal Audit, C&AG, the Department of Education and the Department of Public Expenditure & Reform, or on the issuing of circular letter by the Department of Education or by the Chief Executive in response to business needs. The date of implementation is the date of Chief Executive approval.

9. Ownership and Approval

OWNER	DATE	SIGNATURE
Organisation Support & Development Director	Nov 4, 2024	 Charlie Mitchell (Nov 4, 2024 16:57 GMT)
AUTHORISED/APPROVED BY	DATE	SIGNATURE
Chief Executive	Nov 5, 2024	