msletb
Bord Oideachais agus Oiliúna
Mhaigh Eo, Shligigh agus Liatroma
Mayo, Sligo and Leitrim
Education and Training Board

Mayo, Sligo and Leitrim Education and Training Board

INFORMATION and COMMUNTCATIONS TECHNOLOGY (ICT) ACCEPTAPLE USAGE POLICY

MSLETB,
Corporate Services Department,
Newtown,
Castlebar,
Co. Mayo
F23 DV78

DOCUMENT CONTROL SHEET

Business Unit	Corporate Services, MSLETB
Work Category	ICT
Document Title	Information and Communication Acceptable Usage Policy
Document No.	**V1**

Rev (per footer)	Status	Author(s)	Reviewed By	Approved By	Office of Origin	Issue Date
V1	D01	PB, OR	LC, SC, MMcD, PH.	MSLETB SMT. Noted by Board 12th November 2019.	HQ, Castlebar	12th November 2019

1.0 Table of Contents

Definitions

"**Must**", or the terms "**required**" or "**shall**", refer to an absolute requirement of the policy.

"**Must not**", or the phrase "**shall not**", refer to statements which are an absolute prohibition of the policy.

"**Should**", or the adjective "**recommended**" refers to a statement that should be applied. In certain circumstances, there may exist a valid reason to ignore a particular item. In this case the full implications must be understood and carefully weighed before choosing a different course.

"**Should not**", or the phrase "**not recommended**" mean the specified behaviour should not be performed. There may exist valid reasons in particular circumstances when the particular behaviour is acceptable, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.

1. Scope

This policy applies to any person authorised to have access to Mayo Sligo and Leitrim Education and Training Board (MSLETB) information systems. This includes, but is not limited to, MSLETB employees, contractors to MSLETB and consultants engaged by MSLETB hereafter collectively referred to as users for the purpose of this policy.

This policy applies to all electronic communications systems provided by MSLETB including, but not limited to, internet, intranet, e-mail, personal computers and laptops, digital cameras, PDA's (personal digital assistants) Telecommunication systems and devices. It is the responsibility of both management and staff of MSLETB to ensure that all such tools are used in accordance with this policy.

All users must use common sense and shall conduct themselves in a manner which is appropriate to the execution of duties in the workplace. Breaches of this policy may result in personal liability of users and/or vicarious liability on behalf of MSLETB under many enactments including, but not limited to the following:

- Employment Equality Acts 1998-2015
- Equal Status Acts 2000 - 2015
- General Data Protection Regulations (GDPR) 2018
- The Education and Training Boards Act, 2013
- The Companies Act 2014
- Copyright and Related Rights Act 2000, 2004 and 2007
- Child Trafficking and Pornography Act 1990 1998 and 2004

Other documentation that is relevant to this policy includes MSLETB's policies, such as:

- Grievance Procedure for Staff employed by the ETB
- Prevention policies dealing with Bulling and Harassment/ Sexual Harassment
- Bullying in the workplace
- Data Protection Policy and GDPR Manual
- Records Management Policy
- MSLETB Records Retention Schedule

2. General Computer Usage Regulations and Guidelines

2.1 Contents

All electronic content created or received using equipment or services provided by MSLETB will be regarded as the property of MSLETB.

2.2 Equipment and Resources

All equipment provided by MSLETB for use by staff remains the property of MSLETB. Employees must ensure if any such mobile equipment including, but not limited to, laptops, mobile telephones, etc. is removed from MSLETB's premises it must be kept in a secure environment by the user. If a desktop computer/device is to be removed from MSLETB premises, prior authorisation must be sought from their line manager.

It is the user's responsibility to be informed of the correct operating procedures for the computer resources or products used. A user who is uncertain as to the correct procedure in any situation should obtain clarification before proceeding.

Users must not engage in conduct that interferes with other's use of shared computing resources and/or the activities of other users.

2.2.1 Multi factor authentication

Multi factor authentication (MFA) or two step verification enhances account security by making it more difficult for hackers to sign in – even if they know a user's password. MSLETB use Microsoft Office which has a number of interlinked software packages such as Outlook, Sharepoint and One Note. To ensure that our data is protected, MFA must be installed on all devices.

MFA is a two-step verification process which is enabled when you try to sign into your device. It will ask you for two things; 1. Your password 2. An extra security code.

The security code can be sent in the following forms, and the staff may choose the most convenient for them:

- Call a mobile or other phone.
- Call an office phone (This number can only be entered by administration staff and can include an extension number).
- Text a code to a mobile phone.
- Use the Microsoft Authenticator app on a mobile phone.

Once the security code has been entered correctly, the staff member will have access to their device.

2.3 Security and Passwords

Users must not utilise any other person's access rights or attempt to gain access to resources or data. In exceptional circumstances where access is required, it must be requested in writing by the relevant Manager to MSLETB ICT Support. Users must not attempt to bypass or probe any security mechanisms governing access to the computer systems.

No staff member may misrepresent himself / herself as another individual. This includes using another staff member's username and password.

Passwords must remain confidential to each user and must not be relayed to any other person. MSLETB ICT Support may provide the option to alter any passwords as necessary. Each user carries sole responsibility for security access to his/her computer, laptop or any other electronic device.

2.4 Software Ownership

All software which is provided by MSLETB to a user is licensed and owned by MSLETB and may not be downloaded, stored elsewhere or transferred to another individual by any employee of MSLETB.

Under no circumstances should software be downloaded from the Internet or installed from any other source and used on MSLETB's machines without the prior permission of MSLETB ICT Support. Any breach of these requirements may result in disciplinary action.

2.5 Confidentiality

Users must maintain confidentiality while carrying out their duties and while on MSLETB business.

2.6 Privacy

It should be understood that MSLETB does not provide users with a guarantee to the right to privacy or confidentiality in connection with the use of any technology and users should have no expectation of privacy in the use of MSLETB's ICT resources.

2.7 Monitoring Policy

MSLETB reserves the right and intent to monitor e-mail content and Internet usage to ensure technology is being used properly and to protect MSLETB and its employees from liability under equality, data protection, pornography and copyright legislation. This does not constitute

infringement of any individual rights to personal privacy under the General Data Protection Regulation (GDPR).

Monitoring may be carried out on all Electronic Data including all Web site, Desktop and PC content. This list is not exhaustive. Monitoring developments may change over time. In addition, MSLETB may monitor all PC's for inappropriate images and content.

2.8 Legal Implications of Storing Electronic Data

All information held in electronic format is subject to legislative requirements, as is information held in paper format. These requirements include but are not exclusive to Copyright, Data Protection and Freedom of Information Legislation and the liabilities which may result from breaches of such legislation.

Personal information should contain only information relevant to the individual and to the purpose for which it is being stored. Data must not be used for any other purpose. This data must be maintained in an accurate format and must be altered if the user/Board becomes aware of inaccuracies.

It is an offence to alter or falsify documents in an electronic format or paper / hard copy format. Care must be taken when forwarding or sending information which has been received from a third party or which is specific to another organisation.

Employees should be aware that merely deleting information may not remove it from the system and deleted material may still be reviewed by MSLETB and / or disclosed to third parties.

Please see MSLETB's Data Protection Policy, Record Management Policy and Records Retention Schedule for further information.

2.9 Material of obscene or offensive nature

Users are subject to all legislation regulating the use of MSLETB's IT/ Communications resources. Users must not store, download, upload, circulate or otherwise distribute material containing:

- Any derogatory comment regarding gender, marital status, family status, sexual orientation, religious or political belief, age, disability, race or membership of the travelling community or other categories pursuant to applicable law.
- Any material of a pornographic nature.
- Any material of a paedophilic nature.

- Material containing offensive or foul language.
- Any content prohibited by law.

If an employee receives any offensive, unpleasant, harassing or intimidating messages via e-mail or other computer sources the employee should in the first instance immediately bring it to the attention of their line manager or the HR Manager, who if required, should contact MSLETB ICT Support.

2.10 Virus Protection

Viruses can enter an organisation a number of different ways:

- Unscanned digital storage media (e.g. CDs, DVDs, floppy disks, USB memory sticks) being brought into the organisation.
- E-mails or attachments.
- Downloaded data from the Internet.

Individuals using electronic information must be familiar with and comply with MSLETB's procedures governing usage of USB's, CD's and other software. It is the personal responsibility of each individual to take precautions to ensure that viruses are not introduced into any MSLETB resources or system with which they come into contact.

No computer user may interfere with or disable the Anti-Virus software installed on their desktop PC. Any virus, virus error messages or security incidents must be reported immediately to MSLETB ICT Support at ITSupport@msletb.ie

Do not forward a virus warning to anybody else.

Such warnings are usually hoaxes and are designed to persuade users to delete systems files on their PC; forwarding such a hoax could make MSLETB liable for damage to computer systems outside MSLETB.

3. Email

Employees have an MSLETB e-mail account to facilitate the sending and receiving of business messages between staff and between MSLETB and its clients and suppliers. All communications via email should be done by the organisation e-mail only. While email brings many benefits to MSLETB in terms of its communications internally and externally, it also brings risks to the organisation, particularly where employees use it outside of their MSLETB roles.

Every employee has a responsibility to maintain MSLETB's image, to use electronic resources in a productive manner and to avoid placing MSLETB at risk for legal liability based on their use. It should be remembered that the contents of e-mail are considered as official records for the purpose of legislation such as Freedom of Information Act, National Archives Act, and GDPR.

3.1 Contents

- Messages can carry viruses that may be seriously damaging to MSLETB's systems.

- E-Mail attachments may belong to others and there may be copyright implications in sending or receiving them without permission.

- It has become increasingly easy for messages to go to persons other than the intended recipient and if confidential or commercially sensitive, this could be breaching MSLETB's security and confidentiality as well as Data Protection legislation. Please refer to MSLETB's GDPR manual.

- E-mail is speedy and, as such, messages written in haste or written carelessly are sent instantly and without the opportunity to check or rephrase. This could give rise to legal liability on the part of MSLETB.

- An e-mail message may legally bind MSLETB contractually in certain instances without the proper authority being obtained internally.

- E-mails should be regarded as potentially public information which carries a heightened risk of legal liability for the sender, the recipient and the organisations for which they work.

3.2 Contents

The content of any e-mail must be in a similar style to that of any written communication such as a letter or report as they have the same legal standing. It is important that e-mails are treated in the same manner as any other written form of communication in terms of punctuation, accuracy, brevity and confidentiality. Similarly any written, stored or forwarded and disseminated information must adhere to the guidelines within the GDPR and the Employment Equality legislation and in accordance with the equality policy of MSLETB.

In order to avoid or reduce the risks inherent in the use of e-mail within MSLETB, the following rules must be complied with:

- MSLETB's email disclaimer or a link to same must appear at the end of every e-mail sent from your MSLETB address to an external address.

- The MSLETB name is included in the address of all staff members and is visible to all mail recipients. This reflects on the image and reputation of the organisation, therefore, e-mail messages must be appropriate and professional.

- The signature of an employee must be include the name, department/centre/school, role, and relevant contact details. All signatures must be in the format as set out below:

John Smith | Corporate Services

Mayo, Sligo and Leitrim Education and Training Board
Newtown, Castlebar, Co Mayo
Phone: 094 9024188 | **Email:johnsmith@msletb.ie**

- If employees are using a picture in the email, it must be of the employee only and in an appropriate business format.

- Attachments with personal data must be password protected. Do not send the password in a follow up email.

- Correct spelling and punctuation should be maintained in all communications.

- Corporate e-mail is provided for MSLETB business purposes.

- Occasional and reasonable personal use of e-mail is permitted provided that this does not interfere with the performance, work duties, responsibilities and customer service of MSLETB. It does not support any business other than that of MSLETB and otherwise complies with this policy.

- An e-mail should be regarded as a written formal letter, the recipients of which may be much more numerous than the sender intended. Therefore any defamatory or careless remarks can have serious consequences, as can any indirect innuendo. The use of indecent, obscene, sexist, racist, harassing or other appropriate remarks whether in written form, cartoon form or otherwise is forbidden.

- E-mails must not contain matters which may discriminate on grounds of gender, marital status, family status, age, race, religion, sexual orientation, disability or membership of the Traveller community.

- E-Mails must not contain any inappropriate or lewd content or content likely to cause offence.

- Distribution lists may only be used in connection with MSLETB business. Please note where more than one external email address is being used for the same email, they must be blind copied (BCC). Internally, BCC should be used where appropriate. For example, if sending a reminder to a number of staff to make a return, use BCC so as to not identify who is late, or use BCC when emailing members of a trade union. The decision to BCC should be made on an individual email basis having regard to the context of the mail and its recipients.

- Documents prepared internally for the public or for clients may be attached via e-mail. However, excerpts from reports other than our own may be in breach of copyright and the author's consent should be obtained particularly where the excerpt is taken out of its original context. Information received from a customer should not be released to another customer without prior consent of the original sender. If in doubt consult your manager.

- Do not subscribe to electronic services or other contracts on behalf of MSLETB unless you have express approval to do so.

- If you receive any offensive, unpleasant, discriminatory, harassing or intimidating messages via the e-mail system you must immediately inform your manager or the HR manager.

- Chain mails or unsuitable information must not be forwarded internally or externally.

- MSLETB reserves and intends to exercise the right to review, audit, intercept, access and disclose all messages created, received or sent over the electronic mail system for any purpose or where it deems necessary.

- Notwithstanding MSLETB's right to retrieve and read any electronic mail messages, such messages should be treated as confidential by other employees and accessed only by the intended recipient. Employees are not authorised to retrieve or read any e-mail messages that are not sent to them. However, the confidentiality of any message should not be assumed. Even when a message is erased it is still possible to retrieve and read that message.

- If a user registers with a site or a service using their MSLETB email address the resulting spamming of information may tie up the communications system. Users therefore must not register with a non-business related electronic service using their MSLETB email address without prior permission from their Line Manager and from MSLETB ICT Support, to avoid the release of confidential MSLETB information to third parties and to avoid interference with the communications systems.

4. The Internet / SCORE

Access to the Internet / SCORE (or any intranet service) is provided to staff as necessary solely for the purpose of conducting MSLETB's business. All information and uploaded content on the SCORE is the property of MSLETB.

4.1 Contents

- MSLETB's Internet connections are intended for activities that either support MSLETB's business or the professional development of employees.

- SCORE usage may be monitored on a systematic basis and as deemed necessary by MSLETB.

- Unauthorised downloading of any software programmes or other material is forbidden.

- It is a disciplinary offence to access, download, save, circulate or transmit any racist, defamatory or other inappropriate materials or materials that may discriminate on the

grounds of gender, marital status, family status, age, race, religion, sexual orientation, disability or membership of the Traveller community. This rule will be strictly enforced and is viewed very seriously with potential criminal liabilities arising therefrom.

- It is a disciplinary offence to access, download, save, circulate or transmit any indecent, obscene, child pornographic or adult pornographic material.

- If an MSLETB employee is downloading pornographic images within view of a colleague or forwarding those images to a colleague, this may result in harassment or sexual harassment of the offended parties. Such incidents should be reported to the relevant manager. Apart from any potential offence caused and the inappropriateness of such activity, MSLETB may be vicariously liable for any claims arising from such behaviour.

- Because of the serious criminal implications of accessing child pornography, any employee found to be accessing such information may be summarily dismissed and the matter referred to An Garda Síochána. Furthermore, should an employee be prosecuted under the *Child Trafficking and Pornography Act, 1998,* by engaging in such activities outside the remit of the workplace, MSLETB may find it fitting to invoke disciplinary action.

- The Internet must not be used to pay for, advertise, participate in or otherwise support unauthorised or illegal activities.

- The Internet must not be used to provide lists or information about MSLETB to others and/or to send classified information without prior written approval.

5. Telephone Usage

Access to telephones is intended for MSLETB business purposes only. While reasonable making and taking personal calls is not strictly prohibited, staff are encouraged to keep this to a minimum level. MSLETB reserves the right to monitor the use of the telephone system.

Some mobile phones are provided to staff members for MSLETB business. Personal calls from such phones are permitted but any calls outside the inclusive monthly tariff must be paid for by the staff member.

During office hours, the taking and/or making of calls on personal mobiles is not strictly prohibited however, staff are encouraged to keep such calls to a minimum.

6. Other Electronic Tools

Other electronic equipment (e.g. photocopiers, printers, fax machines etc.) remain the property of MSLETB and as such must be treated with care and used only for MSLETB purposes. Abuse of equipment for personal use or gain may result in the use of the disciplinary procedures and in disciplinary action.

7. Plagiarism

Users should not plagiarise (or use as their own, without citing the original creator) content, including words or images from the Internet. Users should not misrepresent themselves as the author or creator of something found on-line. Research conducted via the Internet should be appropriately cited, giving credit to the original author.

8. Social Media

MSLETB recognises the presence and value of social media tools which can facilitate communication, learning and collaboration. When using these tools, users are expected to communicate with the same appropriate and professional conduct online as offline.

Users should consider rules governing copyright, intellectual property and confidentiality before posting to social media.

Users should be mindful of their privacy settings and postings on personal social platforms. Employees should note that the use of social media in a work setting is subject to the same guidelines and rules as previously outlined in this policy.

9. Removable Media

No non-MSLETB approved removable media such as CD, DVD, USB drive or SD cards etc. that contain data or files may be used without consulting with MSLETB ICT Support.

10. Encryption

All personal data stored on MSLETB mobile devices must be protected by encryption software. It is the responsibility of the staff member to ensure that the data is encrypted and the

encryption software is up to date. This responsibility includes data stored on personal devices. Only encryption software recommended by MSLETB ICT Support should be used.

11. Infringements of Policy

Failure to comply with the policy and guidelines outlined above may result in:

- The withdrawal of e-mail and Internet facilities from the Section, Staff or members involved;
- Initiation of disciplinary procedures and disciplinary action, up and to including dismissal.
- Serious breaches of the policy may result in initiation of criminal or civil proceedings.

12. Responsibilities

Owner	**Responsibilities**
Director of Organisation Support & Development	Revisions and updates to the policy
MSLETB Management Team	Approval of the Policy
All persons who use or have access to MSLETB ICT systems and equipment	Responsible for implementation of the policy.