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.	**V3**

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
V2	D001	OR	SM/SC/SD/CL	EMT: 22nd August Noted by the Board on 20th September 2022	HQ, Castlebar	20th September 2022
V3		OR	PH/SM/BB	EMT: 7th December 2023 Noted by the Board on 12th December 2023	HQ Castlebar	15th December 2023

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, employees (both full and part time), contractors, interns, partners and / or consultants, external individuals and organisations, accessing MSLETB ICT services

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 computing resources include all MSLETB owned, licensed, or managed hardware and software, and use of MSLETB network via a physical or wireless connection, regardless of the ownership of the device connected to the network.

This policy applies to technology administered by MSLETB and is applicable to MSLETB owned computers and devices, connected by wire or wireless to the MSLETB network, and to computers and devices that connect remotely to the MSLETB network services. This also applies to personally owned devices when using MSLETB network resources.

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

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 Bullying and Harassment/ Sexual Harassment

- Bullying in the workplace
- Data Protection Policy and GDPR Manual
- Records Management Policy
- MSLETB Records Retention Schedule

Principles

To comply with the policy, users must follow the principles listed below;

- Use only the computers, computer accounts and computer files for which you have authorisation to access resources needed to perform your stated job function.
- Adhere to the statements in this policy to protect your passwords and to secure resources against unauthorised use or access. For further details on passwords, refer to MSLETB Password Policy.
- You are individually responsible for appropriate use of all resources assigned to you, including the computer, network resources, software and hardware.
- You shall not provide the resources or other forms of assistance to allow any unauthorised person to access MSLETB computers, networks or information.
- MSLETB shall be bound by contractual and licensing agreements with regard to third-party resources. You are expected to comply with all such agreements when using such resources.
- You shall not attempt to access or provide resources to access restricted portions of the network, an operating system, security software or other administrative applications without appropriate authorisation by the system owner or administrator.
- You shall comply with the policies and guidelines for any specific set of resources to which you have been granted access. When other policies are more restrictive than this policy, the more restrictive policy takes precedence.
- You shall not engage in deliberate activity to degrade the performance of information resources; deprive an authorised user access to MSLETB resources; obtain extra resources beyond those allocated; or circumvent MSLETB computer security measures.
- You shall not attempt to bypass any security control unless you have been specifically authorised to do so by the MSLETB ICT Regional Manager or MSLETB Director of OSD.
- You shall not store, share, process, analyse or otherwise communicate corporate information, data or files to external parties, using unauthorised mediums, without prior approval from a line manager in conjunction with the ICT Department. For further clarification on “Authorised Mediums”, contact MSLETB ICT Department. Any security issues discovered will be reported to the head of ICT or their designee for follow-up investigation. Additional reporting requirements can be located within the Compliance section of this policy.

2. General Computer Usage Regulations and Guidelines

2.1.0 Contents

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

2.1.1 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. All such mobile equipment must be returned on request to MSLETB or where there is a change in employment circumstances for example, retirement, termination of employment, change of role/duties, extended leave, etc.

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.

2.1.2 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.

2.2 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. See MSLETB's Password policy for further information.

2.3 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.

2.4 Confidentiality

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

2.5 Privacy

All users of MSLETB network and computing resources should;

- Respect the privacy and personal rights of others.
- Not access or copy another user's email, data, programs or other files without the written permission of MSLETB ICT Regional Manager or Director of OSD.
- Be professional and respectful when using computing systems to communicate with others;

MSLETB reserves the right to access and review information transmitted on MSLETB computing resources as appropriate to ensure the security of MSLETB information assets. This includes investigating performance deviations and system problems (with reasonable cause), for the purpose of determining if an individual is in violation of this policy or, as may be necessary, to ensure that MSLETB is not subject to claims of illegality or misconduct.

Access to a user's files, including, but not limited to, all folders, downloads and emails on MSLETB equipment or information shall only be approved by specific personnel when there is a valid reason to access those files. Authority to access a user(s) files can only be given by the Head of HR / Head of Corporate Services / Director of OSD / Head of ICT / Chief Executive where appropriate, in conjunction with requests and/or approvals from senior members of MSLETB. The Gardaí, with the appropriate verified authority / authorisation may be granted access to files. Such verification should be carried out by the Director of OSD / Chief Executive, as appropriate. 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.

2.6 Monitoring Policy

MSLETB reserves the right and intent to monitor email 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.

2.7 Legal and Regulatory compliance

As a user of MSLETB computing resources, you are expected to act lawfully in the use of these computer resources at all times and in all locations. All users of MSLETB computer resources should ensure that they are fully aware of and understand any of the relevant legislation applicable to IT systems or data, assigned to them in all locations.

As part of the above, a user of MSLETB computing and network resources shall:

- Not engage in activity through any technology medium that may harass, threaten or abuse others.
- Not intentionally access, create, store or transmit material that MSLETB may deem to be offensive, indecent or obscene, or which may be illegal.
- Abide by all applicable copyright laws and licenses. MSLETB may have entered into legal agreements or contracts with providers of software and network resources, which require individuals using them to comply with those agreements. Not use, copy or distribute copyrighted works (including but not limited to web page graphics, sound files, film clips, trademarks, software and logos) unless you have a legal right to use, copy, distribute or otherwise utilise the copyrighted work.

- 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 machines without the prior permission of MSLETB ICT Department

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.

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

If an employee receives any offensive, unpleasant, harassing or intimidating messages via email 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.

2.9 Unacceptable Use

The following are non-exhaustive examples of unacceptable uses:

- Using MSLETB computing services and facilities for personal economic gain, political purposes or otherwise in any way that is in violation of MSLETB Code of Conduct for Staff Members.

- Using MSLETB computing services and facilities in a way that is considered offensive, defamatory, obscene or harassing, including, but not limited to, sexual images, jokes and comments, racial or gender-specific slurs, comments, images or jokes, or any other comments, jokes, or images that would be expected to offend someone based on their physical or mental disability, age, religion, marital status, sexual orientation, or political beliefs, or any other category protected by national or international laws; the use of computing resources to defame or harass any other person is in violation of MSLETB Code of Conduct for Staff Members. and would be subject to the same disciplinary process that is highlighted in the "Compliance" section.

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.
- Emails 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 itservices@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.

For more information on Internet use please see MSLETB's Internet Acceptable Use Policy.

4. The Internet / SCORE

The Internet is constantly evolving in application and content; this policy is not intended to list all forms of acceptable and unacceptable use. Users have the responsibility to use the Internet in an efficient, effective, ethical and lawful manner. They must also follow the same code of conduct expected in any other form of written or face-to-face business communication.

Access to the 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.

For more information on Internet use please see MSLETB's Internet Acceptable Use Policy.

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.

For more information on mobile phone use, please see MSLETB's Mobile Phone Policy.

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.

MSLETB reserves the right to restrict usage of portable storage devices, including USB keys, external hard drives, micro SD cards or even the internal memory on portable devices such as smartphones, tablets and laptops.

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 email 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
Executive Management Team at MSLETB	Approval of the Policy
All persons who use or have access to MSLETB ICT systems and equipment	Responsible for implementation of the policy.