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

INTERNET ACCEPTABLE USE POLICY

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

V1

DOCUMENT CONTROL SHEET

Business Unit	Corporate Services Department, MSLETB
Work Category	ICT
Document Title	MSLETB Internet Acceptable Use Policy
Document No.	V1

Rev (per footer)	Status	Author(s)	Reviewed By	Approved By	Office of Origin	Issue Date
V1	Approved	ETBI ICT Working Group	OR, SM, CL, SD, SC	EMT 22/08/2022 Noted by Board of MSLETB on 20/09/2022	HQ, Castlebar	20/09/2022

1 CONTENTS

2 PURPOSE

The purpose of this policy is to ensure the proper use of the Internet, intranets, extranets, the Web and Internet based resources (to be referred to as the "Internet" by MSLETB's "Users". Usage of these resources is a privilege that is extended to, but not limited to employees (both full and part time), contractors, interns, partners and / or consultants, external individuals and organisations, to be referred to as "Users". This policy applies to any use of the "Internet" from any corporate network(s) or computing devices, including mobile devices, provided by MSLETB or use of internet outside of the organisation networks. It also applies to an employee's personal use of the Internet, as directed below or any other use of.

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.

MSLETB may supplement or modify this policy for users in certain roles. This policy for Internet Usage complements similar MSLETB policies, such as the ICT Acceptable Usage policy. A comprehensive list of ICT policies is located on SCORE Staff intranet, under Staff Policies.

This policy applies to all users of "Internet" resources owned or managed by MSLETB. Individuals covered by the policy include employees (both full and part time), contractors, interns, partners and /or consultants, external individuals and organisations utilising "Internet" resources facilitated MSLETB computing facilities.

3 USER RESPONSIBILITIES

3.1 ACCEPTABLE USE

- The provision of network access and applications (that is, browsers) to access the Internet and Internet based resources is primarily for business-related purposes.
- A discretionary level of personal use of the Internet / Internet-based resources is permitted once same is reasonable and does not constitute unacceptable use (see below) and does not interfere with other business activities or employees' work responsibilities. Personal use of the Internet and corporate infrastructure is a privilege, not a right. It may be revoked at any time. MSLETB accepts no liability for employees' non-business-related activity on the Internet / Internet based resources.
- The Internet provides a plethora of communication mechanisms. All written communication posted to the Internet 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 or posting any communication.
- Access to the Internet and Internet based- resources is acceptable only through corporate-issued applications, such as browsers, IM clients and other tools.

Any software applications sought to be installed by a user must be approved by MSLETBs ICT Department.

3.2 ONGOING TRAINING

All users will be required to undertake ongoing ICT and GDPR awareness training.

3.3 UNACCEPTABLE USE

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

- Accessing Web sites or applications that contain content that can be reasonably interpreted as offensive, harassing, obscene, racist, sexist, ageist or pornographic, or sites that deal with criminal activity, including (but not limited to) those involving or related to illegal drugs, computer hacking/cracking, the creation of malicious software (malware), terrorism, and illegal weapons.
- Using search terms that are likely to result in lists of, or images from, unacceptable Web sites (websites which contain content that can be reasonably interpreted as offensive, harassing, obscene, racist, sexist, ageist or pornographic, or sites that deal with criminal activity, including (but not limited to) those involving or related to illegal drugs, computer hacking/cracking, the creation of malicious software (malware), terrorism, and illegal weapons. Accessing Web sites or applications for personal use that consume excessive network resources for long periods of time, such as multiplayer games, virtual worlds, large file transfers or streaming media.
- Internet use that interferes with the employee's work duties and responsibilities.
- Unauthorised use of copyrighted material from the Internet, such as downloading copyrighted music or movie content via peer-to-peer (P2P) networks or torrent sites.
- Using software or Web sites (often called "anonymisers") that attempt to hide Internet activity for the purpose of evading corporate monitoring.
- Operating a business or any undertaking that offers personal gain or benefit.
- Downloading of computer utilities or tools that are primarily designed for gaining illegal access to other computer systems (usually referred to as hacking or cracking tools).
- Unauthorised attempts to break into, or illegally access or damage, other computer systems or data. (Note: MSLETB is not responsible for an employee's illegal use of the Internet.).
- Forwarding corporate email messages to personal email accounts. This does not include your personal pension, salary or HR information.
- Harassing other users on the Internet or interfering in another user(s) work or use of the Internet. This includes, but is not limited to, the sending of unwanted email, IM or chat messages.
- Publishing, downloading or transmitting content or messages that could be interpreted as offensive, harassing, obscene, racist, sexist, ageist, pornographic or threatening.
- Creating, exchanging, publishing or otherwise distributing in public forums and open communication tools to third parties (for example, via Web email, IM, blog postings, chat rooms, Twitter, virtual representatives and more) any of the following without authorisation: (non-exhaustive list)

1 Product advertisements;

2 Political lobbying;

3 Religious promotion or abasement.

- Transmitting MSLETB confidential information to unauthorised persons or violating MSLETB's Code of Conduct and/or Policies.

- Otherwise using the Internet in a way that increases MSLETB's vicarious, legal and regulatory liability.

Any security issues discovered will be reported to the head of ICT or his/her designee for follow-up investigation. Additional reporting requirements can be located within the Compliance section of this policy.

As a user of MSLETBs Internet / Internet based- resources, you are expected to uphold all Irish legislation and relevant legislation of the European Community. All users of the MSLETB's 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.

3.4 PRIVACY GUIDELINES

Users should have no expectation of privacy in their use of the Internet, including historic searches / browser history. MSLETB maintains the right to monitor and review user(s) Internet activity to ensure compliance with this policy, as well as to fulfil MSLETBs responsibilities under the laws and regulations of the jurisdictions in which it operates.

- MSLETB reserves the right to intercept, monitor, record, review and/or disclose any and all user Internet sessions. Monitoring may be performed with the assistance of URL filtering and/or content-filtering and or monitoring software, or by designated MSLETB employees and/or designated external entities.

- MSLETB reserves the right to alter, modify, reroute or block Internet sessions, as appropriate. This includes, but is not limited to:

  1 Rejecting, quarantining, or removing attachments and/or malicious code from Web pages or FTP file sessions that may pose a threat to MSLETB resources;

  2 Blocking downloadable files and long-lived content, such as music, movies and gaming sessions, that are considered to be of little business value and that involve a significant resource cost;

  3 Rerouting content found in Internet messages or posts (for example, via Web email, IM, blog postings, chat and Twitter) with suspicious content to designated MSLETB employees for manual review.

- Electronic messages and Internet / intranet activity, including draft documents saved to or on MSLETB ICT resources are potentially legally discoverable and admissible as evidence in a court of law.

Any evidence of suspected or alleged illegal activity discovered during monitoring or reviews will be dealt with through MSLETB disciplinary procedure and may lead to a further civil and/or criminal investigation. Refer to MSLETB relevant disciplinary policy for further information.

4 SECURITY

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

- The Internet is the number one transmission vector for malware and viruses. Please exercise extreme caution when surfing the Internet. Even well-respected, branded sites may host malicious content, or may link to sites that do. A good rule of thumb is to be wary of unexpected pop-up windows requesting your permission to take some action (such as download additional browser components). If a Web site is behaving strangely, then close your browser and notify MSLETB's ICT Department immediately.
- Downloading free or "demo" software via the Internet from unknown providers may cause unnecessary security risks, support issues and/or legal liability. If you require software for a specific business purpose, including for evaluation and testing, then please contact MSLETB's ICT Department and\or procurement
- All software running on MSLETB's Systems require a DPIA and DPA to be completed by the Data Protection Office.
- Do not click directly on hyperlinks in email, unless it is an expected communication from a known and trusted source. Normal procedure to get to a site is to open a browser and type the address in the browser address bar. If you do not know the exact addresses, then go to the primary site and use the site navigation to get to the exact page.
- Internet users should not post to any Web site, or use any Internet communications services, to transfer or distribute sensitive data, such as user names, passwords, PPS numbers or account numbers over the Internet without appropriate controls, such as encryption, except in accordance with MSLETB's Data Protection Policy. Sensitive data passed over the Internet could be read by parties other than the intended recipients, particularly if it is clear text traffic. Malicious third parties could potentially intercept and manipulate Internet traffic.
- Attempts to circumvent this policy through the use of anonymous proxies, software or hardware will be considered a violation of the policy.
- **Do not share your network account password** or allow another person to use your account. Do not use another individual's account.
- Do not store corporate information in public storage services unless they are sanctioned by MSLETBs ICT Department.
- Do not use Peer to Peer file sharing networks or torrent sites.
- Do not use remote access tools. For example, Go to My PC, Teamviewer, LogMeIn or Remote Desktop, unless they are supplied and sanctioned by MSLETB's ICT Department Should further clarification be required, contact your line manager or MSLETB's ICT Department.
- Email, IM and other message attachments can contain viruses and other malware. Users should only open attachments from known and trusted correspondents. MSLETB's ICT Department should be notified immediately if a suspicious email / attachment is received.
- 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 MSLETB's ICT Department for further

information. Such approaches may be a phishing attack and these attacks tend to be carried out for the purposes of unlawful exploitation.

- Users are cautioned to only use trusted networks to access the Internet from corporate devices while out of the office. Do not use open consumer wireless (Wi-Fi) networks. Do not attempt to bridge networks or modify firewall settings.

5 OPERATIONAL GUIDELINES

MSLETB employs certain practices and procedures to maintain the security and efficiency of resources, to achieve MSLETB's objectives and/or to meet various regulations. These practices and procedures are subject to change, as appropriate or as required under the circumstances.

5.1 COMPLIANCE

Individuals found to be in breach of this "Internet" Usage 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 MSLETB's ICT Department for full clarification.

6 RELATED POLICIES

Department of Education and Skills circular on Revised Procedures for Suspension and Dismissal of Teachers and Principals (ETBs).

ETBI & Unions Consultative Forum - Disciplinary Procedure for staff employed by Education & Training Boards.

Procedures for principals relating to their work, conduct and matters of professional competence in their role as principals.