Milwaukee School of Engineering
INFORMATION TECHNOLOGY

Acceptable Use Policy

MSOE Information Technology Department
Version 1.1 Effective 7/6/2016, Review Date 7/6/2017

Purpose

The purpose of this policy is to provide users with clear guidance on the appropriate, safe, and legal way in which they can make use of information and IT equipment at MSOE. Users need to be aware of the compliance required with this policy and MSOE's commitment to comply with requirements that all reasonable organizational and technical measures are taken to safeguard its data.

Scope

This Acceptable Use Policy (AUP) applies to the use of all information and IT equipment by MSOE users (including faculty, staff, students, guests, temporary workers, & contractors from other organizations). All users should be aware of their legal obligations and internal policy in respect of information handling.

This policy should be a living document that will change as information use changes in the organization.

All users are expected to have knowledge of at least the portions of this document that are directly related to their role within the organization.

Definitions

1. **Low Risk Information.** This is defined as information that does not require special protective measures.

2. **High Risk Information.** This is defined as information, the loss or breach of which would substantially impair a company.

Policy Statements

1. The primary responsibility for determining changes to the AUP belongs to the Director of IT for MSOE. As such, this person is the executive responsible for managing organizational risk. The policies and rules are a direct consequence of the Information Governance charter.

2. The Director of IT is responsible for ensuring any of MSOE's technical systems can meet our risk management needs as defined by compliance rules. All projects that use or require access to information handling systems (ECM, fileshares, CRM, website, ERP, etc.) must be introduced through the IT department.

    - The Director of IT and the IT department are responsible for ensuring that the project or device is able to comply with all of the security requirements within this policy. Compliance also requires that users are aware of their responsibilities so the Director of IT and the IT department are responsible for ensuring any training needs for IT equipment introduced by the department are met.

3. MSOE's Human Resources and Student Life are responsible for ensuring MSOE rules and policy on acceptable use of equipment are provided as part of MSOE's induction training for new users.

4. All MSOE users, (including temporary or honorary users), who have access to and make use of IT equipment and MSOE IT systems are responsible for using it in accordance with the rules within this policy. In particular, all users must ensure that they use systems in such a way that they ensure student and users confidentiality is maintained.

5. The effectiveness of this policy will be ensured by way of an annual review of reports as part of the Information Technology meeting. It is expected that IT Helpdesk will record any incidents showing non-compliance. Traffic, threat, and application logs are maintained by IT to allow for review of any patterns.

    - New students, staff, and faculty are given a copy of the handbook on recruitment to MSOE. The Computer Misuse policy will provide a link to the complete Acceptable Use Policy.
    - Local experts and departments are expected to audit their own practices from time to time to measure compliance with this policy or in light of future MSOE requirements.

6. MSOE systems must not be used for the creation, transmission, or deliberate reception of any images, data, or other material that is designed or likely to cause offence or needless anxiety, or is abusive, sexist, racist, defamatory, obscene, or indecent. When communicating electronically, users are expected to conduct themselves in an honest, courteous, and professional manner.

7. Users may not use MSOE's IT facilities for commercial activities. This includes, but is not limited to, advertising or running any sort of private business.

    - Use of the internet facility for commercial activities other than in the conduct of MSOE business is prohibited.
    - Users may not use MSOE's IT facilities for advertising or fundraising for commercial or charitable organizations not directly connected with MSOE.

8. Deliberate activities with any of the following consequences (or potential consequences) are prohibited:

    - Corrupting or destroying other users' data.
    - Using systems in a way that denies service to others (e.g. overloading the network).
    - Wasting users effort or computing resources including users involved in the support of those resources.
    - Gaining access to systems that you are not authorized to use.

9. It is permissible for users to send and receive email at work for incidental personal purposes, provided that this does not involve a substantial expenditure of time, or use for profit.

    - Personal email should not add a significant burden to MSOE IT systems.
    - The size of messages, the frequency with which they are sent, and the number of recipients (within MSOE) should not be excessive, and may be monitored to ensure system performance.
    - MSOE has the final decision on what constitutes excessive use. Users must act in accordance with their manager's local guidelines.
    - It is not permitted to write or present views on behalf of MSOE unless authorized to do so.

10. No personally identifiable information or records should be transmitted via email to any external account, this includes personal accounts of MSOE faculty, staff, or students. Any need to share this kind of information should be performed using the system features. End users are not to provide records to users who do not have access to the system or are outside of the campus environment.

- Email queries received from members of the public should always be responded to in writing, not electronically, as it is not possible to be certain that the sender is who they appear to be, or that the message will be read by them.

11. Users should treat email attachments that have been sent unsolicited with extreme caution, especially if the sender is unknown. Viruses are often sent this way. If users are not sure what an attachment is for, or why someone has sent it to them, they should not open it, and seek advice from the IT Service Desk.

    - To intentionally introduce files that cause computer problems is strictly forbidden and could be prosecutable under the Computer Misuse Act 1990.

12. When sending emails to a distribution list:

    - Do not send or forward email to any large group of users unless there is a genuine reason for them to read it.
    - Do not advertise by email.
    - Do not circulate warnings about any virus risk, but consult with the IT Helpdesk.
    - When sending email to external addresses, consider the possibility that this action may inadvertently reveal email addresses to third parties.

13. Forging an email (or any other electronic message), or sending email from any account other than your own without permission may be treated as fraud.

14. Email will not be used for intentional receipt and/or distribution of offensive, obscene, or pornographic material. There is a legal requirement for the Chief Executive to report any computer crime involving child pornography to the police. If users receive an email connected with child pornography, they should seek advice from their manager immediately so that MSOE can take appropriate preventative action.

    - If users receive any pornographic or offensive email, they should not open it or print it. Users must fill in an incident form and let Human Resources know they have received it.
    - If users receive an email containing sexually or racially abusive or discriminatory phrases or material, again they should seek advice from their manager.
    - No users are permitted to distribute email that contains offensive material. Offensive material is defined by MSOE's Equal Opportunity and Harassment Policies and includes hostile text or images relating to gender, ethnicity, race, sex, sexual orientation, religious or political convictions and disability. This list is not exhaustive. Other than instances which demand criminal prosecution, MSOE is the final arbiter on what is or is not offensive material, or what is or is not permissible use of email.

15. Any computing system owned or provided by MSOE is subject to the same conditions of use whether used at home or in the office.

    - Users should take all reasonable care and precautions to ensure safe transport and storage when moving equipment between home or other remote locations and work, keeping it locked and out of sight.
    - Users may be held fully or partially liable for any loss, damage, or theft occurring to MSOE IT equipment whilst in their care. Users are within their rights to refuse to take information and equipment offsite if they feel circumstances mean that they are not able to protect it adequately.
    - All MSOE confidential documentation, whether in paper or data format, should be stored in a secure area of users' homes or the remote location they are working from.

16. The IT department will endeavor to provide all systems with secure access facilities. Access to databases or systems containing important, sensitive, and/or confidential information will be restricted to those users who require access as part of their job function. These may be protected by additional security controls.

    - Where passwords are used, users will be able to select and change their own password by using a minimum of 8 characters (number, letters and symbols).
    - Users should not leave any computer unattended without either logging out or activating a password-protected screensaver. Where a previous user has left their access open, new users must log out from that session first.
    - Users should not add additional password or security measures to any computer or files without first consulting with the IT department.
    - Attempting to remove or bypass any security access on any MSOE computers is strictly forbidden.
    - Passwords are issued for personal use only. They should not be shared or disclosed to anyone else. Users are required to protect their usage against loss, damage, or theft and against possible misuse by others. If a breach of security is recorded, the burden of proof will be with the registered user to show that they are not responsible for the breach.
    - Users should report any known or suspected breaches of information security to the IT Helpdesk for any necessary action to be considered and undertaken.

17. All users are responsible for ensuring that confidential information is stored securely and that appropriate confidentiality is maintained when handling information.

    High Risk Information:

    - Confidential MSOE information should only be stored within a shared folder on the MSOE network, box.msoe.edu, or to a MSOE supplied encrypted laptop or device. At no time should high risk data be stored in any other location.

18. Access to read the document archives will only be granted to users responsible for investigating system failure or system misuse, and then only to look at information as necessary to repair or protect the systems or to investigate use that may be in contravention of this AUP.

    - Document files, web browsing logs, email or voicemail messages, however confidential or damaging, may have to be disclosed in court proceedings or during internal investigations if relevant to the issues being investigated.
    - Access to a user's personal documents, either stored or held in an email mailbox, will only be granted to another user if a written request with appropriate reasons is received from the appropriate Director of MSOE.

19. Infringement of copyright by copying or transmitting copyright material without permission of the copyright holder ("fair use" notwithstanding) is strictly forbidden. The MSOE name/logo may be used only for official MSOE documents and must be used in accordance with Corporate Identity guidelines.

20. The IT department schedules fileserver backups to enable recovery from any system failure.

    - If users do not have access to save their work to a MSOE fileserver, it is essential that they regularly copy any important work either to a backup device, or box.msoe.edu.

21. Changes to enrollment or employment will change the availability of email.

- Employees who cease employment with MSOE, should take responsibility to hand over all MSOE devices and appropriate computer files. Access to the employee email account will be provided to a line manager.
- Employees who retire from employment with MSOE will be given an retiree email account. Access to the original email account will be revoked.
- If users change their job role, IT may hand-over all relevant personal files and email messages to their line manager.
- Students who graduate from MSOE will be given an alumni email account. Access to the original email account will be revoked.
- Students who are not currently enrolled or registered for classes for [90 days] will have their email account deactivated.

22. Access to the Internet is primarily provided for work-related and academic purposes. Reasonable personal use is permitted provided this does not interfere with the performance of duties or adversely affect system performance. MSOE has the final decision on what constitutes excessive use.

    - Personal access to the Internet can be limited or denied by a manager.
    - The IT department has the right to withdraw internet access from any user and globally ban access to any site as appropriate, without warning.
    - Unless specifically authorized, no user may post messages under MSOE's name to any newsgroup or chat room.
    - Unless specifically authorized by the IT department, no user may publish a website under the name of MSOE or featuring its logo.
    - MSOE will not accept liability for personal legal (eg. libel) action resulting from users misuse of the Internet.
    - Access to file downloads will be restricted as necessary by IT to ensure system security.
    - MSOE reserves the right, consistent with local law, to monitor all internet accesses, including but not limited to email and web access. No user should consider information sent/received through the Internet as his/her private information.
    - No user may access, display, or download from internet sites that hold offensive material.
    - Personal/employee identifiable data must not be published in any way on the Internet without the express consent of each and every individual concerned.

23. Do not violate the license agreement by making illegal copies of or providing unlicensed access to MSOE software. Anyone found doing so may be prosecuted under by the software publisher

24. The use of any software package to access, modify, or analyze MSOE's data for either work or personal purposes is forbidden.

25. There should be no expectation that MSOE will pay for personal software. Any information created or used must be stored appropriately based on the storage and retention rules that govern that information source.

Low-Risk Information Specific Policy Statements

1. MSOE allows and encourages the use social media to enhance both its personal visibility and image. Employees are expected to use these media types in a manner that is consistent with their employment contract.

Non-Compliance

Violations of this policy will be treated like other allegations of wrongdoing at MSOE. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable MSOE policies;
2. Termination of employment, contract or enrollment; and/or
3. Legal action according to applicable laws and contractual agreements.

Agreement

Each time you access the MSOE wired or wireless network, you agree to be bound by the Acceptable Use Policy and any additional terms that will apply prospectively to you. You agree to accept notice of posting the new terms via our site on which you accessed these terms. By using this Site you will be deemed to have irrevocably agreed to these Terms.