	DIGITAL MANUFACTURING IRELAND	
Document Title:	Acceptable Use Policy Digital Manufacturing Ireland	
Document Approvers:	**Signature**	**Department**
	Tracey Mannion	Document Control
	Billy Donovan	Information Technology
Version Number:	V1.0	
Effective Date:	31Jul2023	

Contents

1 Purpose & Objectives

The purpose of this policy is to set out the acceptable usage of Digital Manufacturing Ireland's (DMI) data and equipment by staff to ensure information and other associated assets are appropriately protected, used, and handled. Rules for the acceptable use and procedures for handling information and other associated assets should be identified, documented, and implemented. This policy outlines what DMI staff are permitted to do with regards to their information systems and data.

The objective of this policy includes, but is not limited to:

- establish acceptable practices regarding the use of DMI's information resources in order to protect the confidentiality, integrity, and availability of information created, collected, and maintained.
- ensure the security and safety of DMI's IT/OT systems when accessing remotely; and
- ensure the security of the different working environments being used by DMI staff.

2 Scope

The scope of this policy details specific requirements for the use of all physical, computing, and network resources at DMI, including electronic and hardcopy data, information, and information assets. This policy applies to all business units of DMI. It applies to DMI's IT/OT systems and employees, and contractors including authorised third parties (herein referred to as 'Staff').

It can be the case that the assets concerned do not directly belong to DMI, such as public cloud services. The use of such third-party assets and any assets of DMI associated with such external assets (e.g., information, software) should be identified as applicable and controlled. Care should also be taken when a collaborative working environment is used.

3 Governance

The Cybersecurity & IT Support specialist will review this policy on an annual basis. The Cybersecurity & IT Support specialist is responsible for maintenance, updates, control, and communication of the document. It is the responsibility of all DMI staff members within the scope of the policy to follow the appropriate procedures in line with this document.

4 Policy

Personnel and external party users using or having access to DMI's information and other associated assets should be made aware of the information security requirements for handling DMIs information and other associated assets. They should be responsible for their use of any information processing facilities.

4.1 Physical Access to DMI Offices

Staff at DMI are required to obey the physical access controls that are put in place at DMI. These physical access regulations are put in place for the safety of DMI staff, data and premises to avoid any unauthorised access on site. Please refer to the DMI physical access standard for more information.

Staff must:

- adhere to the physical access standard.
- keep their physical access control card safe and always carried visibly with them.
- manage visitors in accordance with the 'DMI Physical & Environmental Security Policy';
- not allow their physical access control card to be used by any other individual.
- report the loss of an access control card immediately to the card issuer in order to deactivate the card; and
- not allow tailgating, which is when an individual, without presenting an access control card, follows an authorised individual into a secured DMI office or other secure location.

4.2 Secure Working Environments

Staff are required to take actions to protect DMI equipment and information when working in any environment (e.g., DMI premises, home, customer sites, when travelling).

Staff must:

- ensure DMI equipment and information are stored in secure lockable furniture, offices or sites when not in use.
- ensure DMI equipment and information is used and sited securely to avoid accidental damage.
- ensure DMI equipment and information are not left unattended in non-secure areas (e.g., public areas, whilst travelling on public transport);
- ensure unattended devices are logged off/locked or protected with a screen locking mechanism controlled by an authenticated unlock method.
- remove sensitive information from workspaces when not in use (e.g., paper records, permitted digital media, other confidential documents);
- dispose of physical sensitive documents in confidential waste bins or shredders; and
- refer to the mobile device policy.

4.3 Access to DMI System

Access to DMI's Systems is controlled by the use of user IDs, passwords and/or authentication tokens. All user IDs and passwords must be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on DMI's Systems. Please refer to the DMI - Logical Access Standard.

Staff must:

- not allow anyone else to use their user ID/token and password on any DMI IT system.
- not use someone else's user ID and/or password to access DMI's systems.
- not leave their password unprotected (e.g., writing it down).
- not use passwords on DMI systems that they use for personal accounts (e.g., personal email).
- not reuse passwords on multiple sites or services.
- not use their DMI user ID as a username or login credential for non-work-related accounts.
- not attempt to access DMI systems or information that they are not authorised to use or access; and
- not store DMI information on any non-authorised DMI, or non-DMI equipment.

4.4 Remote Access

Remote Access is using an electronic device to connect to another computer/network/system from a different location. DMI staff when working remotely must abide by the regulations put in place by DMI. Remote access by staff to DMI systems must be authorised by the relevant party.

Staff must:

- only use authorised remote access solutions.

4.5 General Use of DMI Systems & Information

Staff must use DMI systems and information in accordance with the authorised requirements of their role, and additionally comply with all DMI policies.

Staff must:

- not perform any unauthorised changes to DMI's systems or information.
- not connect any non-DMI authorised device to DMI's network or systems.
- not provide or transfer DMI information or software to any person or organisation outside of DMI unless specifically authorised.
- reasonably limit the use of DMI systems and devices for personal purposes.
- not use a DMI computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
- not reveal account password to others or allow the use of their account by others. This includes family and other household members when work is being done at home.
- not violate the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by DMI.
- not perform unauthorised copying of copyrighted material including, but not limited to, digitization and distribution from copyrighted sources, copyrighted music, and the installation of any copyrighted software for which DMI or the end user does not have an

active licence is prohibited. Users must report unlicensed copies of installed software to the IT department.
- not attempt to prevent or interfere with authorised software installations updates on DMI Systems and devices; and
- only use authorised DMI transfer mechanisms to transfer data internally between DMI systems and externally with third parties.

4.6 Removable Storage Devices

Removable media devices (e.g., memory sticks, CDs, DVDs, and removable hard drives) may only be used in exceptional circumstances where an alternative is not feasible, when authorised by the relevant manager on the IT team and where the device conforms to DMI standards.

Staff must:

- refer to Media Protection Policy.
- only use authorised removable media devices and not attempt to use non-authorised removable media devices.
- not attempt to disable or circumvent any security controls on authorised removable media devices; and
- follow the process for requesting an approved and encrypted USB when required.

4.7 Software Usage

Employees must use only authorised software on DMI's computers. This authorised software must be used in accordance with the software supplier's licensing agreements. All software on DMI's computers must be approved and installed by the IT department.

Staff must:

- only use approved software for DMI business purposes.
- not attempt to use DMI licensed software on non-DMI IT devices; and
- not attempt to install non-authorised software on DMI devices or equipment.

4.8 Internet, Email, Instant Messaging, and Telephony Conditions of Use

Use of DMI's internet access, email, instant messaging, and telephony systems are intended for business use. Personal use is permitted (does not include telephony systems) where such use:

- does not affect the staff members business performance.
- is not detrimental to the DMI in any way.
- does not incur DMI any unauthorised cost.
- is not in breach of terms and conditions of employment; and
- does not place the individual or DMI in breach of statutory or other legal obligations.

All staff are accountable for their actions when using internet access, email, instant messaging, and telephony systems that are provided by DMI.

Staff must:

- use extreme caution when opening email attachments received from unknown senders, which may contain viruses, email bombs, or Trojan Horse codes.
- not use the internet, email, instant messaging, and telephony systems for the purposes of harassment or abuse.
- not use profanity, obscenities, or derogatory remarks in communications.

- not access, download, send, or receive any information in any form, which DMI considers offensive in any way, including sexually explicit, discriminatory, defamatory, or libellous material.
- not use the internet, email, instant messaging, and telephony systems to make personal gains or conduct a personal business.
- not use the internet, email, instant messaging, and telephony systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- not send unprotected sensitive information externally without approval and without using the correct method of transmission for the assigned data classification.
- not forward email to personal email accounts.
- not make official commitments through the internet, email, and instant messaging systems on behalf of DMI unless authorised to do so.
- not download or stream copyrighted material such as (but not limited to) music media files, film, and video files without appropriate approval.
- not in any way infringe any copyright, database rights, trademarks, or other intellectual property; and
- not attempt to download any software from the internet without prior approval of the IT Department.

4.9 Social Media

DMI social media accounts should only be used by the Marketing team. The use of public social media sites to promote organisational activities must only be done on behalf of DMI by the Marketing team. Staff may promote posts/events published by the Marketing team but must refer to the Internet, Email, Instant Messaging, and Telephony Conditions of Use section of this policy for guidance on what content is acceptable.

Unless specifically authorised, the use of organisational email addresses on public social media sites is prohibited. In instances where users access social media sites on their own time utilising personal resources, they must remain sensitive to expectations that they will conduct themselves in a responsible, professional, and secure manner with regard to references to the organisation and staff.

4.10 Malware

DMI installs anti-malware solutions on applicable devices that staff may use to detect, prevent, quarantine, or remove malware.

Staff must:

- not introduce malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- not attempt to remove or disable anti-malware solutions.
- not attempt to prevent or interfere with updates to anti-malware solutions; and
- immediately report any suspected or known malware infections.

4.11 Reporting Security Incidents/Lost or Stolen Items

In the event of a security incident all staff must immediately inform their line manager and report the incident to the IT contact.

4.12 Actions upon Termination of Contract

All DMI information and equipment (e.g., laptops, mobile phones, access tokens, USB storage devices, ID badges) must be returned to DMI at termination of contract.

All DMI information or intellectual property developed or gained during the period of employment remains the property of the DMI and must not be retained beyond termination or reused for any purpose. Please refer to the DMI IT Asset Management Policy and the DMI - Logical Access Process.

4.13 Monitoring and Filtering

Logging and monitoring of DMI system activity will take place where appropriate, and investigations will be initiated where reasonable suspicion exists of a breach of this or other DMI policies.

DMI has the right (under certain conditions) to monitor activity on its systems, including Internet and email, Instant Messaging and Telephony use, in order to ensure systems operate securely and effectively, and to protect against misuse.

Any monitoring will be carried out in accordance with audited, controlled internal processes and in conformance with applicable privacy and data protection legislation.

All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with DMI's disciplinary procedures.

5 Appendix

5.1 Appendix A - Reference Documents

Document Name
DMI - Mobile Device Policy
DMI - Physical Access Standard
DMI - Logical Access Process

Revision History

No #	Revision Description	Date Approved
1.0	New Document	31Jul2023