Acceptable Use Policy

# Information Technology Hardware software and Networks acceptable use policy.

# Version Control

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Amended By | Summary of Change |
| 0.1 | 16/11/2022 | DH | Initial Draft, Purpose centralises current Acceptable use documentation into single cohesive document. |
| 1 | 23/11/2022 | DH | First publish. |
| 1.1 | 04/09/2023 | DH | MLPC Right to monitor systems and network for misuse or abuse. |
|  |  |  |  |

# Introduction/Overview

This policy specifies the requirements for the use of all computing and network resources in Microlink. This includes all electronic information and information assets that are managed by and support Microlink business processes.

As a user of Microlink systems you may handle highly sensitive and restricted information on internal and external networks. It is important that all use of Microlink systems is carried out in a responsible, ethical, and legal manner.

This Acceptable Use Policy is to ensure that information systems provided by or managed by Microlink are used for their intended purpose, maintain confidentiality, integrity and availability of the systems and are used within the bounds of their licences, contractual agreements, and legal obligations.

If a user is in violation of the AUP they may be subject to disciplinary action.

This policy is written in line with Microlink legal obligations under the:

* The Computer Misuse Act (1990)
* The Copyright, Design and Patents Act (1988)
* The Data Protection Act (2018) (known as UK-GDPR)

Contents

[Information Technology Hardware software and Networks acceptable use policy. 1](#_Toc120179650)

[Version Control 1](#_Toc120179651)

[Introduction/Overview 1](#_Toc120179652)

[1. Definitions 3](#_Toc120179653)

[2. Applicability/Scope 3](#_Toc120179654)

[3. Controls 3](#_Toc120179655)

[4. Exceptions 4](#_Toc120179656)

[5. Failure to comply. 5](#_Toc120179657)

[6. Monitoring 5](#_Toc120179658)

# Definitions

|  |  |
| --- | --- |
| *Definition* | *Meaning* |
| *Authentication Details* | *Authentication Details are anything used to prove your identity to a system for example: Username and passwords, PIN, ID badge, Smartcard Yubikey.* |

# Applicability/Scope

 This policy applies to all users of information technology resources owned, managed, or licensed to Microlink PC (UK) Limited.

 Individuals covered by this policy include and are not limited to anyone that is provided access either formally or informally and those who access systems internally or externally including offsite remote workers.

 This policy applies to all systems whether governed and administered centrally by Internal IT or by individual department or individuals themselves

 It also applies to personally owned devices and computers connected by wire or wireless to any Microlink network or system.

# Controls

* 1. To comply with this Acceptable Use Policy individuals covered by this policy **must**:
		1. Use any resources provided by Microlink whether electronic or an analogue for authorised purposes only.
		2. Access only information that they have been authorised to access that is publicly available.
		3. Protect information, electronic or hardcopy, in compliance with ISMS Information Classification & Handling Policy V 2.2.
		4. Protect authentication details such as user ID and passwords and any other authentication and authorisation mechanism from unauthorised use.
			1. *All individuals are responsible for the activity and access carried out using their individual and unique supplied User ID /account credentials.*
		5. Be considerate with their use of company resources and refrain from monopolising systems, overloading networks with excessive data, degrading services, or wasting computer time, connection time, disk space, printer paper, manuals, or other resources.
		6. Restrict personal use to a minimum and minor use that is in line with other Microlink Polices.
		7. Store restricted, confidential, and highly confidential information only on Microlink approved and secured locations.
		8. Transfer/ transport restricted, confidential, and highly confidential information using only approved and secured mechanisms.
		9. Revise password and other authentication mechanisms suspected of compromise.
		10. Report any suspected or identified incidents to the Information Security Manager and IT help desk.
	2. To comply with this Acceptable Use Policy individuals covered by this policy **must** **NOT**:
		1. Attempt to access or use systems, files, or data without permission.
		2. Reveal a password or other authentication mechanism to any other individual, even those claiming to be from Internal IT at the telephone or in person.
		3. Use available resources to decode passwords or access-controlled information.
		4. Attempt to circumvent security controls including network security measures.
		5. Carry out any activity with intent to harm any systems owned and operated by Microlink or not, including spread of viruses or disruption service.
		6. Delete, damage, or make unauthorised changes to Microlink data.
		7. Make, use, store or transmit illegal copies of copyrighted material using microlink computers or systems.
		8. Use email, social media, or any other digital communication services in violation of any laws, or to harass or intimidate another person. For example:
			1. broadcasting unsolicited messages
			2. repeatedly sending unwanted mail
			3. using someone else’s name or User ID
			4. Waste shared computing or network resources, for example:
				1. by intentionally placing a program in an endless loop
				2. printing excessive amounts of paper
				3. sending chain letters or unsolicited mass mailings
			5. Place links to sites which:
				1. facilitate illegal or improper use
				2. contain Copyrighted materials or facilitate in its distribution
				3. display pornographic material
		9. Post messages which would be in contempt of court. Use Microlink’s systems or networks for commercial purposes outside of those that are not for fill Microlink business. For example, by selling access to your User ID or by performing work for profit with Microlink resources in a manner not authorised by Microlink.
		10. State or imply that you speak on behalf of Microlink or use any of its trademarks, logos without authorisation.
		11. Violate any laws that govern the use of IT resources such as but not limited to Computer Misuse Act (1990), Copyright, Design and Patents Act (1988), Data Protection Act (2018)
		12. Use “auto-forward” rules to send business e-mail to a non-Microlink email account.
		13. Store confidential data on local drives, flash drives, or other portable or external media.
		14. Use company resources for personal use.

# Exceptions

 No exception may be made regarding any legal obligations to any applicable laws. Any exception must be logged in the Exception log and approved by CISO and reviewed periodically.

# Failure to comply.

 If an individual is found to be in violation of the Acceptable Use Policy, Microlink will take disciplinary action, including restriction of and possible loss of network privileges or more serious consequences, up to and including termination of employment.

 This policy is subject to change as contractual obligations and statute laws evolve.

# Monitoring

* 1. Microlink reserve the right to ensure that computer systems used for business use are appropriately monitored to ensure.
		1. They are not abused.
		2. Are being used in line with this, and other policies laid out by Microlink PC.
		3. Are used only for business purposes.
	2. This policy should be reviewed and updated at least annually

|  |  |
| --- | --- |
| Name:  | Michael Moore |
| Position: | Legal Counsel |
| Date: |  |
| Signature: |  |