



1. Information Security Policy

Introduction

- 1.1 This information security policy is a key component of MHCCC management framework. It sets the requirements and responsibilities for maintaining the security of information within MHCCC. This policy may be supported by other policies and by guidance documents to assist putting the policy into practice day-to-day.

Purpose

- 1.2 This policy is intended to support MHCCC business objectives and, without undue restrictions, protect its staff, clients, contractors, third parties and the business from illegal or damaging events or actions by individuals, either knowingly or unknowingly.
- 1.3 The objective of this policy is to define the MHCCC's procedures to protect the confidentiality, integrity, and availability of MHCCC's information assets, its reputation, and the safety of all its stakeholders. Everyone who works in or with the Company has a duty and a responsibility to comply with these policies.

Applicability

- 1.4 The policy applies to the use of all MHCCC IT equipment and information systems belonging to or managed by the company, including but not limited to laptops, workstations, servers, networks, supporting infrastructure, telephones, telephony systems, mobile devices (such as smart-phones), removable media, third-party systems and any cloud-based infrastructure, platforms, or services.
- 1.5 This policy is applicable to all MHCCC staff both permanent and temporary, contractors, agency workers and any third parties who provide services. It is the responsibility of all such individuals to read and understand this policy, and to conduct activities in full accordance with it. If there is any uncertainty, employees should consult the centre coordinator.

Aim and Scope of this policy

- 1.6 The aims of this policy are to set out the rules governing the secure management of our information by:
- preserving the confidentiality, integrity and availability of our business information.
 - ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies.
 - ensuring an approach to security in which all members of staff fully understand their own responsibilities.
 - creating and maintaining within the organisation a level of awareness of the need for information.
 - detailing how to protect the information assets under our control.

- 1.7 This policy applies to all information/data, information systems, networks, applications, locations and staff of MHCCC or supplied under contract to it.

Responsibilities

- 1.8 Ultimate responsibility for information security rests with the Management Group but the Centre Coordinator shall be responsible for managing and implementing the policy and related procedures.

Responsibility for maintaining this Policy, the business Information Risk Register and for recommending appropriate risk management measures is held by the Centre Coordinator. Both the Policy and the Risk Register shall be reviewed by the Management Group at least annually.

- 1.9 The Centre Coordinator is responsible for ensuring that their staff, and contracts are aware of: -

- The information security policies applicable in their work areas.
- Their personal responsibilities for information security.
- How to access advice on information security matters.

- 1.10 All staff shall comply with the information security policy and must understand their responsibilities to protect the Centre's data. Failure to do so may result in disciplinary action.

The Centre Coordinator shall be individually responsible for the security of information within their business area.

Each member of staff shall be responsible for the operational security of the information systems they use.

- 1.11 Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity, and availability of the information they use is maintained to the highest standard.

Access to the organisation's information systems by external parties shall only be allowed where a contract that requires compliance with this information security policy is in place. Such a contracts shall require that the staff or sub-contractors of the external organisation comply with all appropriate security policies.

- 1.12 To ensure compliance, the following is needed:

- Appoint a manager with specific responsibilities for security – the risk owner.
- Appoint a person responsible for day-to-day security.
- Identify individuals responsible for specific information assets such as: family information, staff, or finance information. They need to be able to understand the threats likely to compromise the information.
- Ensure that all individuals with designated security responsibilities undertake appropriate training for their role.

We are committed to reviewing our policy and good practice annually.

Name:	Signature:	Date:
Daleep Mukarji		
This policy was last reviewed on: 4 th February 2025		