The Order of Malta Volunteers – Information Security Policy

(registered company no. 09801949, registered charity no. 1164242)

POLICY REFERENCE	
Function	For information and guidance
Status	Approved and issued
Scope	Trustees, OMV Committee, Volunteers,
Owner	Eddie Pease
Date originally adopted by Board	November 2025
Version	1.0
Date of last full Board review	November 2025
Date for next annual Policy holder review	November 2026

Introduction

1. The purpose of this Information Security Policy is to protect OMV's information assets from all threats, whether internal or external, deliberate or accidental. The OMV Committee and Trustees are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets owned or processed by their organisation in order to provide secure applications to users, comply with legal, regulatory and contractual obligations.
2. This policy applies to all volunteers, trustees, and third-party service providers who have access to OMV's information systems and data. It covers all information assets, including but not limited to digital data and physical documents.

3. The Charity must publish this Policy on its website.

Information Security Objectives

4. The OMV is committed to achieving the following information security objectives:
    - Protect the confidentiality of information by ensuring that access is limited to authorised individuals.
    - Maintain the integrity of information by preventing unauthorised modification or destruction of data.
    - Ensure the availability of information by maintaining reliable and resilient information systems.
    - Comply with all relevant legal, regulatory, and contractual requirements related to information security.
    - Foster a culture of security awareness and continuous improvement within the organisation
5. To achieve the above objectives, the OMV will adhere to the following principles:

- Access to information assets will be granted based on the principle of least privilege and need-to-know.
- Multi-factor authentication (MFA) must be enabled where applicable.
- Regular access reviews will be conducted.
- Confidential and Restricted data must be encrypted at rest and in transit.
- Information security incidents will be promptly reported, investigated, and mitigated.
- Examples of reportable incidents include phishing attempts, unauthorized system access, and data leaks.

Roles & Responsibilities

6. OMV Trustees: responsible for this policy and ultimately responsible for ensuring that it is implemented in the organisation
7. OMV Committee: responsible for the implementation of this policy across the organisation
8. IT Lead: responsible for implementing and maintaining technical security controls, including access controls, encryption, and network security.

Training & Awareness

9. Committee Members and Activity Leads should have annual training on this policy.

Policy Enforcement

10. The Trustees take a proactive approach to risk management and regularly reviews its risk register to ensure that it remains fit for purpose.

Legal & Regulatory Compliance

11. The OMV will comply with all relevant legal, regulatory, and contractual obligations concerning information security, including but not limited to data protection laws, industry-specific regulations, and contractual agreements with clients and partners.

10. Remote Work & Cloud Security

12. Use of personal email accounts by the OMV Committee and Activity organisers is prohibited.
13. OMV Committee and Activity organisers must not store OMV data either on unauthorized cloud storage services or on personal devices.
14. Cloud providers used by the OMV must meet ISO 27017 & ISO 27018 (Cloud Security & Privacy) standards.

Review

15. The Policy Owner must keep up to date with relevant legislation and Charity Commission guidance and update this Policy whenever necessary. The Board of Trustees must approve the revised version.

16. The Policy Owner must review the Policy annually and either submit a revised policy for approval by the Board of Trustees or confirm in writing to the Chairman of Trustees that the current version of this Policy is still fit for purpose.

17. The Board of Trustees must formally review and re-approve this Policy every five years.