# IT-POL-05.1 Information Security Policy

| | | | |
|---|---|---|---|
| **Version Number** | 4 | **Developed by** | Head of IT Simon Kane |
| **Approval Date** | 28/03/23 | **In Consultation With** | |
| **Classification Type - (Confidential, Restricted, Internal use only, None)** | | | Internal Use Only |

## 1. Introduction

The information we use to support our service users and manage the organisation exists in many forms, it may be stored electronically, printed or written on paper or spoken in conversation.

Whatever forms the information takes, or the means by which it is shared or stored, it should be treated as an important asset and be appropriately protected from unauthorised access, modification or loss.

It is Framework's policy to protect information regarding service users (clients), donors, staff, volunteers, partners and the organisation from security risks that might have an unfavourable effect on our operations, our professional standing or an individual's personal privacy.

Security risks include people obtaining or disclosing information inappropriately, information being altered, whether deliberate or accidental and information not being available when required.

To provide assurance to our customers, staff, donors, service users (clients), and management that Framework's security measures meet information security best practice and are working correctly, our ISO 27001:2013 aligned information security practices include an Information Security Management System encompassing the following:

- Identification and classification of information assets
- Appointment and training of information asset owners.
- Undertaking risk assessments and implementing appropriate technical, managerial and environmental controls.
- Publication of information security policies.
- Complying with the information security requirements requested by customers.
- Establishing an Information Security Forum,
- Providing information security training to all staff, including directors, staff, volunteers and contractors
- Establishing an information security incident reporting and management process.
- Reviewing and monitoring information security controls throughout our supply chain.
- Complying with relevant legislation, including the Data Protection Act 2018, and the European General Data Protection Regulations
- Undertaking technical, policy and procedure audits of our information security controls.
- Continually improving our information security position and reporting the status to senior management

# IT-POL-05.1 Information Security Policy

## 2. Responsibilities

The CEO owns this Information Security Policy and is committed to the implementation of it.
*Objectives for Framework's Information Security Management System are aligned with the strategic plans of the organisation, defined by the Senior Management Team. These objectives are subject to a 'cascade' process to set objectives at all levels within the organisation.*

The Information Security Forum is collectively responsible for ensuring that information within Framework is adequately protected and for allocating sufficient resources.

Information asset owners are responsible for classifying their information and ensuring that the risks to their assets are identified and addressed.

Line management are to ensure that information security is included within the processes they are responsible for and ensuring that their staff play their part in protecting the information in their care.

All staff are required to observe company polices, attend information security awareness training and report information security incidents or weaknesses to the Head of Information & Technology.

The Head of Information & Technology is responsible for providing information security guidance and where necessary investigating information security incidents.

The Audit & Risk Management Committee receives copies of the Information Security internal audit reports.