

Information Handling Policy

(ISO 27001:2022 Organisational Controls – Clauses 5.10,
5.12, 8.10)

Author	Greg Nott
Version	2.0
Date Created	06/05/2023
Last Update Date	14/05/2024
Document Control	Released
Document ID	230506-IMS-POL-InformationHandling-V2
Security Classification	Public

Table of Contents

Information Handling Policy	1
Approval.....	3
Review.....	3
Change History.....	3
Associated Documents.....	3
Scope.....	4
Purpose.....	4
Exceptions.....	4
Policy Statements.....	4
Information Classification and Handling	4
Access Control.....	5
Information Handling Procedure	5
Reuse of Information Assets	5
Information Security awareness and Training.....	6
Personal Identifiable Information (PII).....	6
Storage of Personal Identifiable Information (PII)	6
Printing of Personal Identifiable Information (PII)	6
Retention and Destruction of Personal Identifiable Information (PII)	6
Incoming and Outgoing of Physical Media Containing PII Data.....	7
Responsibilities	7
Head of Information Security.....	7
Employee's	7
Compliance	7
Policy Review	7

Approval

Author	Issue	Approved By	Date
Paul Langan	1.0	Simon Naylor	23-Aug-23
Greg Nott	2.0	Paul Langan	16-May-24

Review

Reviewer	Review Criteria	Issue	Date
Greg Nott	ISO 27001:2022	1.0	06-May-23
Paul Langan	Review & Rebrand	2.0	16-May-24

Change History

Author	Change	Issue	Date
Paul Langan	Creation	1.0	06-May-23
Greg Nott	Review & Rebrand	2.0	16-May-24

Associated Documents

Document	Version
230419-IMS-POL-InformationExchange-V2	2.0
230501-IMS-POL-DataDestructionPolicy-V2	2.0

Scope

This document is part of the Integrated Management System (IMS) for ARO and is consistent with the standards listed below and describes the Information Handling Policy adopted by ARO.

- ISO 27001:2022 – Information Security Management Systems
 - ISO 27017:2015 – Code of Practice for Cloud Services
 - ISO 27018:2020 – Code of Practice of Personally Identifiable Information (PII)
- ISO 9001:2015 – Quality Management System
- DSPT (Data Security and Protection Toolkit) for the NHS.
- Cyber Essentials Plus

This policy applies to all employees, contractors, and third-party entities who have access to the organisation's information assets, including but not limited to electronic, physical, and verbal information.

Purpose

The purpose of this policy is to establish guidelines and responsibilities for the handling of information within the organisation. This policy aims to ensure the confidentiality, integrity, and availability of information assets, and to comply with relevant legal, regulatory, and contractual requirements.

Exceptions

- Any exceptions to the application of this policy or where controls cannot be adhered to MUST be presented to the Head of Information Security or a member of the management team.
- All exceptions to this policy MUST be maintained on a risk register for accountability, traceability, and security governance reporting to senior management.

Policy Statements

Information Classification and Handling

- All information assets must be classified according to their sensitivity level, using a classification scheme approved by the organisation. The classification scheme should define the appropriate controls and handling requirements for each level of sensitivity. The classification scheme adopted by ARO is:
 - **Confidential** - Company confidential, information will be made available and distributed strictly on a need-to-know basis.
 - **Commercial In Confidence** - Documents that are Shared/Co-authored with partners that contain proprietary information.
 - **Public** - General Release
 - **Internal** - Internal Company information not deemed to be confidential or public. Open to all staff.
- Employees must handle information assets in accordance with their classification level and the associated handling requirements. This includes proper storage, transmission, and disposal of information assets.
- Information assets must be protected against unauthorised access, disclosure, alteration, and destruction throughout their lifecycle. Access controls and encryption mechanisms should be

implemented as appropriate.

- Classification of information assets such as information processing systems and information categories will be identified and documented in the Information Asset Register. All documents produced by the organisation must clearly be labelled with their classification unless the document is deemed 'Public' in which case no label is required, although it is still recommended to label these documents wherever possible.

Access Control

- Access to information assets must be granted based on the principle of least privilege. Employees should only be given access rights necessary to perform their job functions.
- User accounts must be created, modified, and revoked based on predefined procedures. All user accounts must be regularly reviewed for appropriateness and promptly deactivated upon termination or change of job roles.
- Passwords must be strong, unique, and compliant with the Password Management Policy. The use of multifactor authentication is mandatory wherever possible, especially for accessing sensitive information assets.

Information Handling Procedure

- Mobile devices and removable media must be appropriately protected to prevent unauthorised access, loss, or theft. Encryption and password protection should be used when storing sensitive information on such devices.
- All client information is held electronically in secure databases having no direct external access.
- Access to all classified information (i.e., information that is of value to the business) will be restricted consistently with this procedure. Procedures and systems are in place to implement appropriate access controls, to ensure that information is stored and transported securely and is not lost or corrupted (e.g., Management of Removable Media, Information Exchange, Change Control and Backup).
- ARO specific documents held within Office 365 (Cloud based) access is dependent upon the user's role in the company. Access can be either: Read-Only, editable, or full control.
- Database specific information is held in a secure DBMS can only be accessed directly by authorised personnel.
- Information must be deleted when no longer required. Where required (i.e., sensitive and/or client) must follow the Data Destruction Policy.
- Data Exchange must follow the Data Exchange Policy.

Reuse of Information Assets

- Any information assets that are being reused needs to be handled in line with the Secure Disposal and Reuse of Equipment Policy.

Information Security awareness and Training

- Employees must receive regular information security awareness and training to enhance their understanding of information handling requirements, risks, and responsibilities.
- New employees and contractors must undergo information security training as part of their onboarding process.
- Records of information security training and awareness sessions must be maintained for audit and compliance purposes.

Personal Identifiable Information (PII)

- In respect of personal identifiable information (includes PID – Patient Identifiable Data, processed within SDCS) when an individual gives consent for his/her personal information to be shared a change request must still be raised and authorised. This is also the same when implied consent is given. When using PII data, the staff members should be aware of the Caldicott Principles which are:
 - Is the purpose for using the data justified.
 - Only use identifiable information if necessary.
 - Use the minimum required.
 - Access should be on a strict need to know basis.
 - Everybody must understand their responsibilities.
 - Understand and comply with the law.
 - The duty to share information can be as important as the duty to protect of confidentiality.
- When using PII data consideration should be given to pseudonymisation and anonymisation.

Storage of Personal Identifiable Information (PII)

- All PII data stored by ARO will be encrypted at rest (This does not apply to client media which ARO has no access to).
- All Patient Identifiable Data (PID) processed within SDCS will be held in a secure safe haven (usually within a TRE).

Printing of Personal Identifiable Information (PII)

- Printing of PII shall only be conducted when absolutely necessary to produce hard-copy such as for letters or labelling and only basic data (i.e. name, address) should be printed.
- Where PII can be processed electronically it should not be printed.
- It is the policy of ARO that no PID is to be printed under any circumstances.

Retention and Destruction of Personal Identifiable Information (PII)

Please refer to the following policies

- Record Retention Schedule

- Data Destruction Policy

Incoming and Outgoing of Physical Media Containing PII Data

- Wherever possible ARO will ensure PII data will only be received to/from via sFTP (or any secure data transfer method approved by NHS England).
- Where ARO needs to transfer PII data by physical media a change request will be raised to authorise and track this.

Responsibilities

Head of Information Security

- Establishing and approving the information classification scheme and associated handling requirements.
- Allocating adequate resources to implement and maintain information handling controls.
- Monitoring compliance with this policy and taking appropriate corrective actions.
- Reviewing and updating the policy periodically to reflect changes in the organisation's information handling practices and regulatory requirements.

Employee's

- Adhering to the information handling requirements specified in this policy.
- Reporting any suspected or actual information security incidents to the appropriate authority.
- Participating in information security awareness and training programs.
- Following the established procedures for the handling of information assets.

Compliance

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contract.

Policy Review

This policy shall be reviewed and revised as necessary, but at least annually, to ensure its ongoing suitability and effectiveness.