Information Classification& Security Policy

Approval Sign-off			
Author	**Role**	**Signature**	**Date**
Robert Forster	Information Technology Manager		22 February 2022
Approver	**Role**	**Signature**	**Date**
Abiola Bamigbade	Head of Quality & Regulatory Affairs		22 February 2022

SUMMARY

Kays Medical is certified to BS EN ISO 27001:2013 – Information Security Management System and are required to comply with the requirement to implement and maintain a quality management system. In order to preserve the appropriate confidentiality, integrity and availability of information assets, the Organisation must make sure they are protected against unauthorised access, disclosure or modification. This is not just critical for assets covered by the Data Protection Act, and the primary and secondary data used for all business conducted across the Organisation by the Organisation. Different types of information require different security measures depending upon their sensitivity.

The Organisation's information classification standards are designed to provide information owners with guidance on how to classify information assets properly and then use them accordingly.

This guidance - developed in accordance with the Security and Data Protection Policies - includes classification criteria and categories, as well as rules for the delegation of classification tasks.

This policy does not form part of any employee's contract of employment and we may amend it at any time.

1. CONTENTS

2. PURPOSE AND SCOPE

The purpose of this document is to provide a fully comply with current regulations and legislation relating to the protection of information and data and to ensure business continuity and minimise business damage by preventing and minimising the impact of security incidents. In particular, information assets must be protected in order to ensure:

1. Confidentiality i.e., protection against unauthorised disclosure
2. Integrity i.e., protection against unauthorised or accidental modification
3. Availability as and when required in pursuance of the Organisation's business objectives.

3. DEFINITIONS

Information Classification Definitions- The following table provides a summary of the information classification levels that have been adopted by the Organisation. These classification levels explicitly incorporate the Data Protection Act's (DPA) definitions of Personal Data and Sensitive Personal Data, as laid out in the Data Protection Policy.

Confidential-Confidential information has significant value for the Organisation, and unauthorised disclosure or dissemination could result in severe financial or reputational damage to the Organisation, including fines from the Information Commissioner's Office. Data that is defined by the Data Protection Act as Sensitive Personal Data falls into this category. Only those who explicitly need access must be granted it, and only to the least degree in order to do their work (the 'need to know' and 'least privilege' principles). When held outside the Organisation, on mobile devices such as laptops, tablets or phones, or in transit, all documents of any type of classification are never stored on the local drive and access to such information can only be secured through: (i) accessing the desktop which is protected behind a secure logon process, and (ii) thereafter accessing the drives, which are encrypted for the stored information.

Restricted- Restricted information is subject to controls on access, such as only allowing valid logons from a small group of staff. 'Restricted' information must be held in such a manner that prevents unauthorised access, i.e. on a system that requires a valid and appropriate user to log in before access is granted. Information defined as Personal Data by the Data Protection Act falls into this category. Disclosure or dissemination of this information is not intended, and may incur some negative publicity, but is unlikely to cause severe financial or reputational damage to the Organisation. Note that large datasets of 'Restricted' information may become classified as Confidential, thereby requiring a higher level of access control.

Internal Use- Internal use information can be disclosed or disseminated by its owner to appropriate members of the Organisation, consultants and contractors, as appropriate by information owners without any restrictions on content or time of publication.

Public-Public information can be disclosed or disseminated without any restrictions on content, audience or time of publication. Disclosure or dissemination of the information must not violate any applicable laws or regulations, such as privacy rules. Modification must be restricted to individuals who have been explicitly approved by information owners to modify that information, and who have successfully authenticated themselves to the appropriate computer system.

Designating information as 'Confidential' involves significant costs in terms of implementation, hardware and ongoing resources, and makes data less mobile. For this reason, information owners making classification decisions must balance the risk of damage that could result from unauthorised access to, or disclosure of, the information against the cost of additional hardware, software or services required to protect it.

4. PREREQUISITES

Not applicable

5. RESPONSIBILITIES

Activity	Responsibility
✓ They are responsible for assessing and classifying the information they work with, and applying the appropriate controls. They must respect the security classification of any information as defined, and must report the inappropriate situation of information to the ISMS Manager as quickly as possible. ✓ Responsible to safeguard assets, including locations, hardware, software, systems or information, in their care and to report any suspected breach in security without delay, direct to the ISMS representative.	Members of Staff or Contractors
Information Owners are responsible for assessing information and classifying its sensitivity. They should then apply the appropriate controls to protect that information. Information ownership can be delegated: see the Security Policy.	Information Owners
Responsible for providing the mechanisms or instructions for protecting electronic information while it is resident on any the Organisation owned or controlled system.	Data Processors
✓ Responsible for providing the instructions for the protection and preservation of records, physical or electronic. Responsible for advising and recommending information security standards on data classification. ✓ Day-to-day responsibility for procedural matters, legal compliance, maintenance and updating of documentation, promotion of security awareness, liaison with external organisations, incident investigation and management reporting. ✓ Day-to-day responsibility for data protection rests. ✓ Day-to-day responsibility for technical matters, including technical documentation, systems monitoring, technical incident investigation and liaison with technical contacts at external organisations.	Information Systems Manager

6. PRECAUTIONS AND SAFETY

Not Applicable.

7. EQUIPMENT, MATERIALS AND CONSUMABLES REQUIRED

Workstation with access to Q Drive on Kays network

8. PROCEDURES

8.1 Examples of Security Level Definitions

8.1.1 Confidential

8.1.1.1 Normally accessible only to specified and / or relevant members of staff. This includes DPA-defined Sensitive personal data including:

- racial/ethnic origin
- political opinion
- religious beliefs
- trade union membership
- physical/mental health condition
- sexual life
- a criminal record including when used as part of primary or secondary research data.

8.1.1.2 Salary information
8.1.1.3 Individuals' bank details
8.1.1.4 Draft research reports of controversial and/or financially significant subjects.
8.1.1.5 Passwords
8.1.1.6 Large aggregates of DPA defined Personal Data including elements such as name, address, telephone number
8.1.1.7 HR system data
8.1.1.8 The Organisation central and/or client data
8.1.1.9 Interview transcripts, client databases or other research records involving individually identifiable sensitive subject to significant scrutiny in relation to appropriate exemptions/public interest and legal considerations.

8.1.2 Restricted

Normally accessible only to specified/relevant members of the Organisation staff. DPA-defined Personal Data (information that identifies living individuals) including:

- ✓ home/work address
- ✓ age
- ✓ telephone number
- ✓ schools attended
- ✓ photographs including where used as part of primary or secondary research contained in research databases, transcripts or other records
- ✓ draft reports, papers and minutes
- ✓ systems.

Subject to significant scrutiny in relation to appropriate exemptions/public interest and legal considerations.

8.1.3 Internal Use

8.1.3.1 Normally accessible only to members of staff, consultants and contractors. DPA-defined Personal Data (information that identifies living individuals) including:

- Internal correspondence
- Information held under license
- Company policy and procedures.

Subject to scrutiny in relation to appropriate exemptions/public interest and legal considerations. Public

Accessible to all members of the public including:

8.1.3.2 Annual accounts
8.1.3.3 The information available on the Organisation website or through Organisation publications.

8.2 Granularity of classification

The sets of information being classified should, in general, be large rather than small. Smaller units require more administrative effort, involve more decisions and add to complexity, thus decreasing the overall security.

8.3 Information Retention

There may be minimum or maximum timescales for which information must be kept. These may be mandated in a research or commercial contract. Other forms of information retention may be covered by environmental or financial regulations.

9. REFERENCES

ISO 27001: 2013 Information Security Management

General Data Protection Regulation (EU) 2016/679

10. VERSION HISTORY

Change History			
Version	**Date** *(dd mmm yyyy)*	**Author / Editor**	**Details of Change** *(Brief detailed summary of all updates/changes)*
01	06 Jan 2021	Jon Mackay	Document created
02	03 Aug 2021	Jon Mackay	Update template.
03	22 February 2022	Robert Forster	SOP name changed from "Information Classification Policy" to "Information Classification& Security Policy". Responsibility table extended.

11. APPENDIX

Not Applicable.