

# Mendlesham Medical Group

## Information Governance Policy

Policy Title / Reference	Author	Owner
Information Governance Policy	Emma Cooper, Kafico Ltd	Mendlesham Medical Group

Version	Revision author	Version comments
1	Emma Cooper, DPO	Jan 18

### 1. Contents

2.	Introduction .....	2
3.	Statutory Mandatory Framework .....	2
4.	Accountable Parties .....	3
	Practice Manager .....	3
	Senior Information Risk Owner (SIRO) .....	3
	Information Asset Owners (IAOs) .....	3
	Caldicott Guardian Function .....	4
	Data Protection Officer (DPO) .....	4
	All Staff .....	4
5.	Openness .....	4
6.	Privacy and Information Rights .....	5
7.	Information Security .....	5
8.	Information Quality and Records Management .....	6
9.	Associated Protocols .....	6
10.	Audit Schedule .....	6
11.	Review .....	7

# Mendlesham Medical Group

## 2. Introduction

Information Governance (IG) is a set of multi-disciplinary structures, policies, procedures, processes and controls implemented to manage information at an organisational level. Information Governance supports Mendlesham Medical group's immediate and future regulatory, legal, risk, environmental and operational requirements.

Information is a vital asset, both in terms of the commercial development and the efficient management of services and resources. It plays a key part in governance, service planning and performance management.

It is therefore of critical importance to ensure that information is appropriately managed, and that policies, procedures and management accountability and structures provide a robust governance framework for information management.

Mendlesham Medical Group recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. Mendlesham Medical group fully supports the principles of clinical and corporate governance and recognises the power of public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients, the public and staff and commercially sensitive information. Mendlesham Medical Group also recognises the need to share information with commissioners, partners and other third parties in a controlled manner consistent with the established lawful basis.

This overarching Information Governance Policy and the associated protocols sets out Mendlesham Medical Group's policy with respect to the governance of;

- Privacy
- Information and Cyber Security
- Data Quality and Records Management

## 3. Statutory Mandatory Framework

This policy serves to support Mendlesham Medical Group to navigate and comply with the complex framework within which Information Governance operates.

This framework includes but is not limited to;

- NHS Act 2006
- Health and Social Care Act 2012
- Data Protection Act 2018

# Mendlesham Medical Group

- Human Rights Act 1998
- Common Law Duty of Confidence
- Computer Misuse Act 1990
- General Data Protection Regulations (EU) 2016/679
- Mental Health Capacity Act 2005
- Children Act 1989
- DH Records Management Code of Practice
- DH Information Security Code of Practice
- DH Confidentiality Code of Practice

## 4. Accountable Parties

### The Practice Manager

The Practice Manager has overall responsibility for Information Governance at Mendlesham Medical Group. As the senior accountable officer, he/she is responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to provide the necessary assurance to internal and external stakeholders.

The Practice Manager has a particular responsibility for ensuring that Mendlesham Medical Group meets its corporate legal responsibilities, and for the adoption of internal and external governance requirements.

### Senior Information Risk Owner (SIRO)

The SIRO;

- leads and fosters a culture that values, protects and uses information for the success of the organisation and benefit of its customers.
- owns the organisation's overall information risk policy and risk assessment processes and ensuring they are implemented consistently by Information Asset Owners / Administrators.
- Owns the organisation's information incident management framework

### Information Asset Owners (IAOs)

The IAO will;

Hold local responsibility for information risk management, devolved to the relevant directors, department leads by the SIRO. Business function leads within Mendlesham Medical Group

# Mendlesham Medical Group

have overall responsibility for the management of risks generated by their information assets and are supported on a daily basis by Information Asset Administrators.

## Caldicott Guardian Function

The Caldicott Guardian will;

- Produce procedures, guidelines and protocols to support staff in the appropriate management of patient information
- Provide a point of escalation and specialist advice for staff with respect to information sharing, acting as the conscience of the organisation
- bring to the attention of the relevant manager any occasion where the appropriate procedures, guidelines and protocols may have not been followed and raise concerns about any inappropriate uses made of patient information where necessary.

## Data Protection Officer (DPO)

The DPO Will;

- inform and advise the organisation and its employees about their obligations to comply with the data protection legislation.
- monitor compliance with the data protection legislation, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, patients etc).

## All Staff

All staff, whether clinical or administrative, who create, receive and use data have information governance responsibilities. Employees have a contractual and legal obligation to read and comply with all company policies and to attend mandatory training to support the appropriate management of information.

## 5. Openness

Non-confidential information related to Mendlesham Medical Group and its services will be available to the public through a variety of media, in line with Mendlesham Medical Group's overall commitment to transparency

Mendlesham Medical Group will adopt and maintain clear procedures and arrangements for liaison with the press and broadcasting media

# Mendlesham Medical Group

Mendlesham Medical Group will adopt and maintain an Information Rights and Access Protocol and a Freedom of Information Protocol to provide guidance for handling queries from data subjects and the public.

## 6. Privacy and Information Rights

Mendlesham Medical Group is committed to the privacy of its patients, staff and the public. Mendlesham Medical Group will undertake or commission annual assessments and audits of its compliance with privacy legislation and will adopt and maintain protocol for completion of Data Protection Impact Assessments.

Mendlesham Medical Group regards all Personal Data relating to staff as confidential except where national policy on accountability and openness requires otherwise

Mendlesham Medical Group will adopt and maintain protocols to ensure compliance with the Data Protection Act, General Data Protection Regulations, Human Rights Act and the common-law confidentiality

Mendlesham Medical Group will establish and maintain protocols for the controlled and appropriate sharing of personal information with other agencies, taking account of relevant legislation (e.g. Data Protection Act, Human Rights Act).

Mendlesham Medical Group will ensure that contractual or best practice documents are in place for routine sharing of information between sharing partners.

## 7. Information Security

Mendlesham Medical Group will adopt and maintain protocols for the effective and secure management of its information assets and resources

Mendlesham Medical Group will undertake or commission annual assessments and audits of its information and IT security arrangements

Mendlesham Medical Group will promote effective information and cyber security practice to its staff through policies, procedures and training

Mendlesham Medical Group will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of information and cyber security

# Mendlesham Medical Group

## 8. Information Quality and Records Management

Mendlesham Medical Group will establish and maintain protocols and procedures for information quality assurance and the effective management of records

Mendlesham Medical Group will undertake or commission annual assessments and audits of its information quality and records management arrangements

Managers will be expected to take ownership of, and seek to improve, the quality of information within their services

Wherever possible, information quality will be assured at the point of collection

Data standards will be set through clear and consistent definition of data items, in accordance with national standards.

Mendlesham Medical Group will promote information quality and effective records management through protocols, procedures/user manuals and training

## 9. Associated Protocols

This policy should be read in conjunction with;

- Risk Management Policy
- Change Management Policy
- Information Rights and Access Protocol
- Information Sharing and Privacy Protocol
- Information Lifecycle and Data Quality Protocol
- Information / Cyber Security Protocol
- Information Incident Protocol
- Information Risk and Audit Protocol
- Data Protection Impact Assessment Protocol
- Freedom of Information Protocol

## 10. Audit Schedule

Compliance with this policy will be audited and the results fed into the Plan, Do, Check, Act Cycle described in the Information Risk and Audit Protocol.

Policy Section	Compliance Evidence	Monitoring Method	Frequency
<b>4 Accountable Parties</b>	The most senior members of the organisation are regularly appraised of	IG Audit	Quarterly

# Mendlesham Medical Group

	internal and external governance status and requirements including resource requirements		
<b>4 Data Protection Officer</b>	Changes within the organisation are subject to a Data Protection Impact Assessment	IG Audit	Quarterly
<b>4 Data Protection Officer</b>	The DPO is being made aware of all processing activities across the organisation	Processing Activities Log	Quarterly
<b>6 Privacy and Information Rights</b>	The organisation has an effective infrastructure in place to ensure privacy and to give effect to the information rights of individuals	IG Audit	Quarterly
<b>7 Information Security</b>	The organisation has an effective infrastructure in place to ensure information security	IG Audit	Quarterly
<b>8 Information Quality and Records Management</b>	The organisation has an effective infrastructure in place to ensure information security	IG Audit	

## 11. Review

This policy will be reviewed every two years or sooner where necessary.