**

**MINSTER MEDICAL GROUP**

**Data Security Policy**

**MINSTER MEDICAL GROUP**

**Minster Medical Centre**

**Parkwood Health Centre**

**Sheppey Healthy Living Centre**

**Tel: 01795 877714 Fax: 01795 877715**

|  |  |
| --- | --- |
| Name | Helen Gaylor |
| Approval Date | 11.02.2020 |
| Review Date | 11.02.2021 |

# Policy

The Information Security Policy outlines the approach, methodology and responsibilities for preserving the confidentiality, integrity and availability of Minster Medical Group information. It is the overarching policy for information security and supported by specific technical security, operational security and security management policies. It supports the 7 Caldicott principles and 10 data security standards. This policy covers:

* Information Security Principles.
* Governance – outlining the roles and responsibilities.
* Supporting specific information security policies – Technical Security, Operational Security and Security Management.
* Compliance Requirements.

## Information Security Principles

The core information security principles are to protect the following information/data asset properties:

* Confidentiality (C) – protect information/data from breaches, unauthorised disclosures, loss of or unauthorised viewing.
* Integrity (I) – retain the integrity of the information/data by not allowing it to be modified.
* Availability (A) – maintain the availability of the information/data by protecting it from disruption and denial of service attacks.

In addition to the core principles of C, I and A, information security also relates to the protection of reputation; reputational loss can occur when any of the C, I or A properties are breached. The aggregation effect, by association or volume of data, can also impact upon the Confidentiality property.

For the NHS, the core principles are impacted, and the effect aggregated, when any data breach relates to patient medical data.

[This section describes the main information properties and the additional issues of the impact on confidentiality of aggregated data, either by association or volume, and the requirement to consider reputational impacts.]

## Governance – Roles and Responsibilities

### All Staff

Information Security and the appropriate protection of information assets is the responsibility of all users and individuals are expected at all times to act in a professional and responsible manner whilst conducting Minster Medical Group business. All staff are responsible for information security and remain accountable for their actions in relation to NHS and other UK Government information and information systems. Staff **shall** ensure that they understand their role and responsibilities, and that failure to comply with this policy may result in disciplinary action. This will be reinforced by yearly mandatory training.

### Caldicott Guardian

The Caldicott Guardian is responsible for ensuring implementation of the Caldicott Principles and Data Security Standards with respect to Patient Confidential Data.

### Data Protection Officer

The Data Protection Officer is responsible for ensuring that Minster Medical Group and its constituent business areas remain compliant at all times with Data Protection, Privacy & Electronic Communications Regulations, Freedom of Information Act and the Environmental Information Regulations. The Data Protection Officer **shall**:

* Lead on the provision of expert advice to the organisation on all matters concerning the Data Protection Act, compliance, best practice and setting and maintaining standards.
* Provide a central point of contact for the Act both internally and with external stakeholders (including the Office of the Information Commissioner).
* Communicate and promote awareness of the Act across the <insert name of organisation>.
* Lead on matters concerning individual’s right to access information held by Minster Medical Group and the transparency agenda.

### Information Asset Owners

The Information Asset Owners (IAOs) are senior/responsible individuals involved in running the business area and **shall** be responsible for:

* Understanding what information is held.
* Knowing what is added and what is removed.
* Understanding how information is moved.
* Knowing who has access and why.

[The aim of the IAO role is to have a nominated role or person to be responsible for the management and control of information assets. Within larger organisations this is normally from a dedicated role. For smaller organisations, this role is likely to be undertaken by the Information Governance Lead.)

### Senior Responsible Owners

The Executive Manager is responsible for ensuring that this policy and information security principles **shall** be implemented, managed and maintained in their business area. This includes:

* Appointment of Information Asset Owners (IAO) to be responsible for Information Assets in their area(s) of responsibility.
* Awareness of information security risks, threats and possible vulnerabilities within the business area and complying with relevant policies and procedures to monitor and manage such risks
* Supporting personal accountability of users within the business area(s) for Information Security
* Ensuring that all staff under their management have access to the information required to perform their job function within the boundaries of this policy and associated policies and procedures.

## Supporting Policies

The Information Security Policy is developed as a pinnacle document which has further policies, standards and guides which enforce and support the policy. The supporting policies are grouped into 3 areas: Technical Security, Operational Security and Security Management and are shown in the diagram overleaf. The Information Security Policy is closely aligned to the NHS Information Governance Strategy and relies upon, and supports, the Minster Medical Group Physical and Personnel Security policies.

### Technical Security

The technical security policies detail and explain how information security is to be implemented. These policies cover the security methodologies and approaches for elements such as: network security, patching, protective monitoring, secure configuration and legacy IT hardware & software.

### Operational Security

The operational security policies detail how the security requirements are to be achieved. These policies explain how security practices are to be achieved for matters such as: data handling, mobile & remote working, disaster recovery and use of social media.

### Security Management

The security management practices detail how the security requirements are to be managed and checked. These policies describe how information security is to be managed and assured for processes such as: information security incident response, asset management and auditing.

[For larger organisations, the overleaf diagram on supporting policies will result in separate documents for each policy; however, for smaller organisations these may be combined or covered under a coverall for each area (technical, operational and security management). Some organisations will have outsourced their IT to a supplier or provider and therefore the information security policy and supporting policies will need to focus on the requirements and conditions to be implemented by the contacted provider.]



[The above diagram should be produced to reflect ‘The Tree’ or ‘Framework’ of policies that will be utilised by the organisation.]

## Compliance Requirements

### Legislation

Minster Medical Group is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation **shall** be devolved to employees and agents of Minster Medical Group who **may** be held personally accountable for any breaches of information security for which they **may** be held responsible. Minster Medical Group **shall** comply with all relevant legislation appropriate; this includes but is not limited to:

* Data Protection Act 1998
* Freedom of Information Act 2000
* Health & Social Care (Safety & Quality) Act 2015
* Computer Misuse Act 1990

### Review

This policy **shall** be reviewed at least annually by the reviewers noted within the Reviewers section of this policy. The Information Security Officer **shall** be responsible for ensuring the review is conducted in good order and follows due process for approval.

The Information Security Officer is accountable for providing the results of ongoing reviews of information security implementation across Minster Medical Group This includes support to the annual Information Governance Toolkit return.