|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Version | Author | Owner | Rationale | Date | Review date |
| 1.3 | S Forrester-Wild | J Johnson | * Addition of version page * Update of document | 12 December 2023 | 01 June 2023 |

# Information Security Principles

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

|  |  |  |
| --- | --- | --- |
| Confidentiality | C | Protect data from breaches, unauthorised disclosures, loss and unauthorised viewing |
| Integrity | I | Retain the integrity of data by not permitting it to be modified without consent |
| Availability | A | Maintain the availability of 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.

# Terminology

|  |  |
| --- | --- |
| Term | Meaning/Application |
| SHALL | This term is used to state a **Mandatory** requirement of this policy |
| SHOULD | This term is used to state a **Recommended** requirement of this policy |
| MAY | This term is used to state an **Optional** requirement |

# Governance – Roles and Responsibilities

## All Staff

Information Security and the appropriate protection of information assets is the responsibility of all users. Individuals are always expected to act in a professional and responsible manner whilst conducting the practice’s 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.

## Senior Information Risk Owner

The Senior Information Risk Owner (SIRO) is accountable for information risk within the practice and advises on the effectiveness of information risk management across the organisation. All Information Security risks shall be managed in accordance with the practice’s Risk Management Policy.

## Information Governance Lead

The Information Governance Lead (IG Lead) is responsible for the day-to-day operational effectiveness of the Information Security Policy and its associated policies and processes. The IG Lead **shall**:

* Lead on the provision of advice to the organisation on all matters concerning information security, compliance with policies, setting standards and ensuring best practice
* Provide a central point of contact for information security
* Ensure the operational effectiveness of security controls and processes
* Monitor and co-ordinate the operation of the Information Security Management System.
* Be accountable to the SIRO and other bodies for Information Security across the practice
* Monitor potential and actual security breaches with appropriate expert security resource.

## Caldicott Guardian

The Caldicott Guardian is responsible for ensuring implementation of the Caldicott Principles and Data Security Standards with respect to patient confidential data.

### Caldicott Principles

|  |  |
| --- | --- |
| Principle 1 | Justify the purpose(s) for using confidential information |
| Principle 2 | Do not use personal confidential data unless it is necessary |
| Principle 3 | Use the minimum necessary personal confidential data |
| Principle 4 | Access to personal confidential data should be on a strict need-to-know basis |
| Principle 5 | Everyone with access to personal confidential data should be aware of their responsibilities |
| Principle 6 | Comply with the law |
| Principle 7 | The duty to share information can be as important as the duty to protect patient confidentiality |
| Principle 8 | Inform patients and service users about how their confidential information is used |

## Data Protection Officer

The Appointed Data Protection Officer (DPO), as defined in the GDPR 2016 and UK GDPR 2021.

The Data Protection Officer is responsible for ensuring that the practice and its constituent business areas always remain compliant 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 both internally and with external stakeholders, including the ICO
* Communicate and promote awareness of the Act across the Practice
* Lead on matters concerning individuals right to access information held by the practice and the transparency agenda

## Information Asset Owners

The Information Asset Owners are senior/responsible individuals involved with the 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

# Supporting Policies

The Information Security Policy has further policies, standards and guides which support this policy. The supporting policies are grouped into 3 areas: Technical Security, Operational Security and Security Management. The Information Security Policy supports the practice’s 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 and 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.

# Legislation

The practice 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 the practice who may be held personally accountable for any breaches of information security for which they may be held responsible.

The practice shall comply with all relevant legislation appropriate and this includes but is not limited to:

* Data Protection Act 2018
* Freedom of Information Act 2000
* Health & Social Care (Safety & Quality) Act 2015
* Computer Misuse Act 1990
* General Data Protection Regulation (GDPR) 2016 & UK GDPR 2021

# Audit

Audits will be performed as part of the practice’s ongoing Audit Programme. The Information Governance Lead shall ensure appropriate evidence and records are provided to support these activities at least on an annual basis