Oak Vale Medical Centre

Data Security & Protection Policy
Version No: 1

The purpose of the Data Security & Protection Policy is to support the 7 Caldicott Principles, the 10 Data Security Standards, General Data Protection Regulation (2016), Data Protection Act (2018), the common law duty of confidentiality and all other relevant legislation. Data Protection is a fundamental right and the Practice will embrace the principles of data protection by design and default.

Document type	Data Security & Protection Policy
Date approved	**March 2019**
Next review date	**March 2021** or sooner should legislative change require.
Applies to	All Staff

Contents

1.0 SCOPE

The Practice is committed to adhering to the 10 National Data Security Guardian Standards (NDG) in order to ensure the protection and security of all Data which the Practice processes.

This policy was developed in conjunction with the guidance outlined in NHS Digitals Information Security Policy, Data Protection Act 2018 and advice from the Information Commissioner's Office following the General Data Protection Regulation (GDPR) which came into force on 25th May 2018.

2.0 INTRODUCTION

This policy outlines the approach, methodology and responsibilities for preserving the confidentiality, integrity and availability of Oak Vale Medical Centre 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.

3.0 DUTIES, ACCOUNTABILITIES AND RESPONSIBILITIES

This policy applies to all those working within the Practice, in whatever capacity. A failure to follow the requirements of the policy may result in investigation and management action being taken, in line with the Practice's disciplinary policy and procedure.

The Information Governance Lead/Practice Manager must make their staff aware of the Data Security & Protection Policy at the earliest possible opportunity.

3.1 Practice 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 business. All staff are responsible for the information security and remain accountable for their actions in relation to NHS and other UK Government information and information systems. It is mandatory that staff ensure 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.

3.2 Information Governance Lead

The Information Governance(IG) Lead must give their full backing to all the guidelines and procedures as set out and agreed. They must ensure that their staff are aware and adhere to the policy requirements.

The IG Lead is 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.

All Senior Manager's are individually 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.

Practice manager and computer manager are accountable for information risk within the Practice and advise the Partners on the effectiveness of information risk management within the Practice.

All Information Security risks shall be managed in accordance with the Practices Risk Management Policy.

3.3 Information Security Lead

The Information Security Officer is responsible for the day to day operational effectiveness of the Data Security and Protection Policy and its associated policies and processes. The Information Security Lead shall:

- Lead on the provision of expert 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 Practice Manager/Senior Partner for Information Security with the Practice.
- Monitor potential and actual security breaches with appropriate expert security resource.

3.4 Caldicott Guardian/IG Lead

The Caldicott Guardian/IG Lead is responsible for:

- Ensuring implementation of the Caldicott Principles and Data Security Standards with respect to Patient Confidential Data.
- Ensuring that the Practice processes satisfy the highest practical standards for handling patient information and provide advice and support to Practice staff as required.
- Ensuring that patient identifiable information is shared appropriately and in a secure manner. The Caldicott Guardian will liaise where there are reported incidents of person identifiable data loss or identified threats and vulnerabilities in Practice information systems to mitigate the risk.

The aim of the Caldicott Guardian is to ensure the organisation implements the Caldicott principles and data security standards; there is no need to appoint a Caldicott Guardian, but there is a need to have an Information Governance lead (sometimes referred to as a Caldicott lead) who, if they are not a clinician, will need support from a clinically qualified individual.

3.5 Data Protection Officer (DPO)

The Data Protection Officer is responsible for ensuring the Practice remains 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 Practice on all matters concerning the Data Protection Act, compliance, best practice and setting and maintaining standards.
- Inform and advise the organisation and its employees of their data protection obligations under the GDPR.
- Monitor the organisation's compliance with the GDPR and internal data protection policies and procedures. This will include monitoring the assignment of responsibilities, awareness training, and training of staff involved in processing operations and related audits.
- Advise on the necessity of data protection impact assessments (DPIAs), the manner of their implementation and outcomes.
- Serve as the contact point to the data protection authorities for all data protection issues, including data breach reporting.

The DPO will be independent and an expert in data protection. The DPO will be the Practice's point of contact with the Information Commissioner's Office

4.0 POLICY

The Data Protection & Security Policy outlines the approach, methodology and responsibilities for preserving the confidentiality, integrity and availability of the Practices' 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. (see section 3)
- Supporting specific information security policies – Technical Security, Operational Security and Security Management.
- Compliance Requirements.

4.1 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.

4.2 Supporting Policies

The Data Security & Protection 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 Data Security & Protection Policy is closely aligned to the NHS Information Governance Strategy and relies upon, and 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: back-up policy – see computer and data security policy.

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: acceptable use policy, computer and data security policy & business continuity and disaster recovery policy.

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: Data breach and incident reporting policy

See Appendix One for a framework of policies.

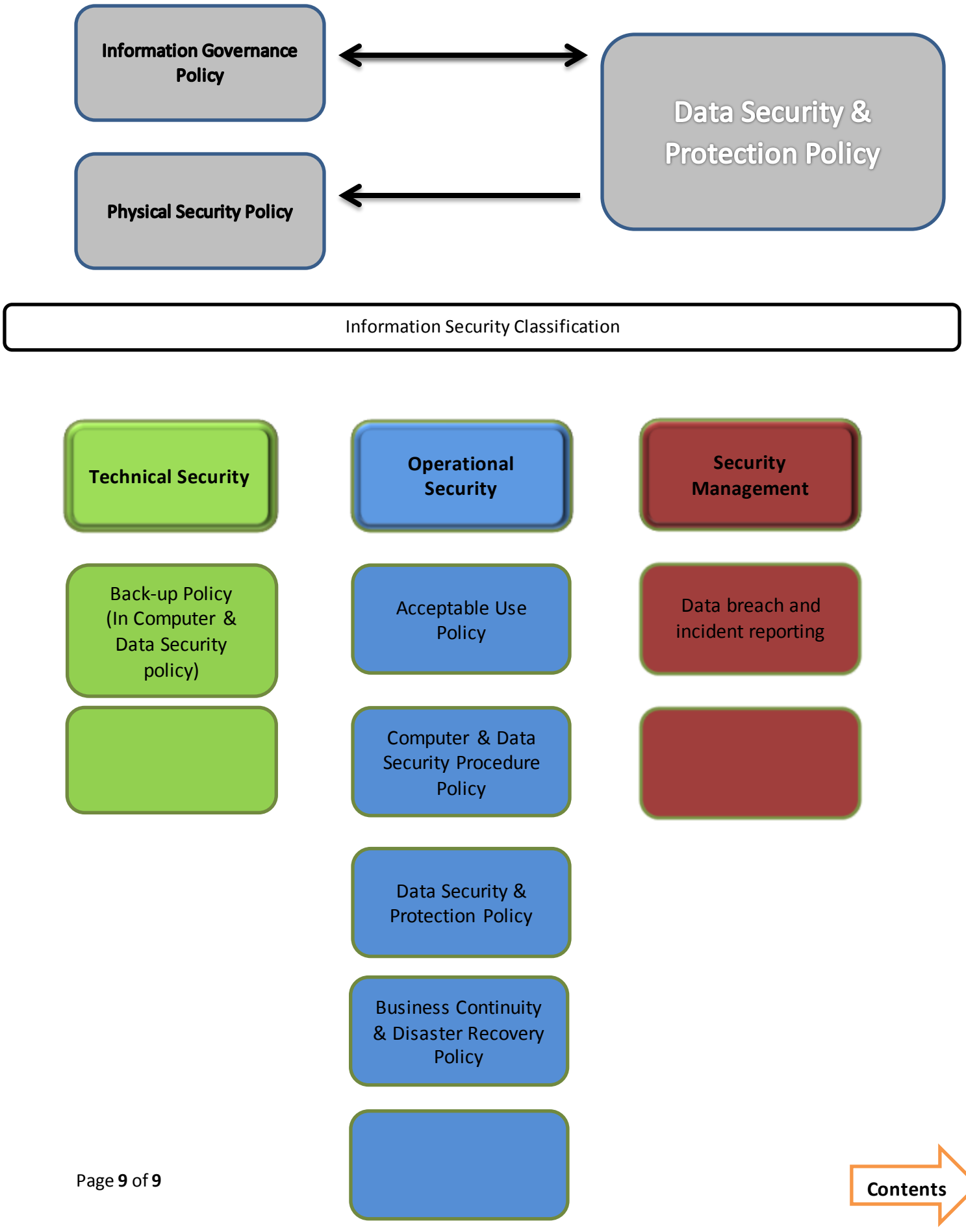
4.3 Compliance Requirements

Legislation relevant to this policy;
The Practice will comply with all relevant legislation; this includes but is not limited to:

- The Data Protection Act 2018
- The General Data Protection Regulation
- The NHS Confidentiality Code of Practice 2003
- Common Law Duty of Confidentiality
- Freedom of Information Act 2000
- Health & Social Care Act 2016
- Computer Misuse Act 1990

5.0 REFERENCES

Author	Year	Title	Edition	Place of Publication
NHS Digital	2017	Information Security Policy	1st	UK


Information Governance Policy
Physical Security Policy
Data Security & Protection Policy
Information Security Classification
Technical Security
Back-up Policy (In Computer & Data Security policy)
Operational Security
Acceptable Use Policy
Computer & Data Security Procedure Policy
Data Security & Protection Policy
Business Continuity & Disaster Recovery Policy
Security Management
Data breach and incident reporting