Liscard Group Practice

|  |
| --- |
| **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. |

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.

**Introduction**

This policy outlines the approach, methodology and responsibilities for preserving the confidentiality, integrity and availability of Liscard Group Practice 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.

**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 Practice Manager must make their staff aware of the Data Security & Protection Policy at the earliest possible opportunity.

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.

**IG Lead**

The Information Governance (IG) Lead (Dr Staples) 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.

The Practice Manager and Partners, are individually responsible for ensuring that this policy and information security principles shall be implemented, managed and maintained in their business area.

**Caldicott Guardian/IG Lead**

The Caldicott Guardian/IG Lead (Dr Staples) 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.

**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 Officershall:

* 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.

**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.

## 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.

**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