|  |
| --- |
| **Information Governance Policy**  **Version No: 2**  **Document Summary:**  This Information Governance Policy reinforces the Practice’s commitment to progressing the Information Governance Agenda at the Practice.  The Information Governance Policy sets out the principles by which the confidentiality, integrity and availability of person identifiable and corporate information will be managed at the Practice. |

|  |  |  |
| --- | --- | --- |
| **Document status** | Approved | |
| **Document type** | Policy | **local** |
| **Approving body** | MMDA Information Governance Steering Group | |
| **Date approved** | 21/09/2021 | |
| **Date implemented** | 30/09/2024 | |
| **Review date** | **30/09/2027** | |
| **Accountable Officer** | Dr M Northey- Greenbank Surgery | |
| **Practice Review** | 22/06/2023 MN | |
| **Policy Author** | Camilla Bhondoo - Head of Risk Assurance and Data Protection Officer | |
| **Target audience** | All staff and workers | |
| **Key words** | Information Governance, Data Protection, Confidentiality, Information | |

Document Control

**[Author to complete all sections apart from Section 4 & 5]**

|  |  |  |  |
| --- | --- | --- | --- |
| **Section 1 – Document Information** | | | |
| **Title** | **Information Governance Policy** | | |
| **Directorate** | | Informatics | |
| **Brief Description of amendments** | | | |
| Click here to enter text.  ***Please state if a document has been superseded.*** | | | |
| **Does the document follow the Practice agreed format?** | | | Yes |
| **Are all mandatory headings complete?** | | | Yes |
| **Does the document outline clearly the monitoring compliance and performance management?** | | | Yes |
| **Equality Analysis completed?** | | | Yes |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Section 2 – Consultation Information** | | | | |
| **Consultation Completed** | | Yes | | |
| **Consultation start date** | Click here to enter a date. | | **Consultation end date** | Click here to enter a date. |

|  |  |  |
| --- | --- | --- |
| **Section 3 – Version Control** | | |
| **Version** | **Date Approved** | **Brief Summary of Changes** |
| 7.0 | 20/03/2017 |  |
| 8.0 |  | * Additional information and further background on what IG is and the frameworks to aid compliance – **Section 1 (Introduction)** * Purpose of policy explained and how the Practice aim to protect information – **Section 2 (Statement of Intent)** * Moved from Section 2 and entered into own section – **Section 4 (Policy Principles)** * Removal of Definitions section as terms described require own section i.e. openness * Section 4.1 Openness and Information Sharing moved from further down the policy and completely updated – **Section 4.1** * Information on the UK GDPR Principles added and further information on how the Practice complies with the principles (establishing a lawful basis and Privacy Notice) – **Section 4.2 (Legal compliance)** * Information Security section moved to Section 4.3 * Information Quality Assurance changed from Records Management and moved to Section 4.4 * Change to duties and responsibilities. Further detail provided for the following: DPO, IAO, IAA, IG Team, , Staff and workers - **Section 5 (Duties, Accountabilities and Responsibilities)** * Reference to the DSPT training requirement and how IG mandatory is made available –**Section 6 (Training and Guidance)** * Definition of breach as per UK GDPR added, brief description of the IG incident process and scoring of incident including escalation process **– Section 7 (IG Incident Reporting and Management)** * New section added on DSPT, what it is, the sections within that require completion and who monitors compliance i.e. IGSG and Risk Management Council - **(Section 8 DSPT)** * Detailed added as previously marked as ‘none’ – **(Section 10 References / Bibliography)** * List of associated IG documents added – **(Section 11 Practice Related Policy/Procedure)** * New section added on when policy review is required – **(Section 12 Review)** |
|  | Click here to enter a date. |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Section 4 – Approval** *– To be completed by Document Control* | | | | |
| **Document Approved** | |  | | |
| **Assurance provided by Author & Chair** | |  | | |
| **Date approved** | Click here to enter a date. | | **Review date** | Click here to enter a date. |

|  |  |  |
| --- | --- | --- |
| **Section 5 – Withdrawal** *– To be completed by Document Control* | | |
| **Reason for withdrawal** | |  |
| **Assurance provided by Author & Chair** | |  |
| **Date Withdrawn:** | Click here to enter a date. | |

Contents

[Document Control 2](#_Toc82182529)

[1. SCOPE 5](#_Toc82182530)

[2. INTRODUCTION 5](#_Toc82182531)

[3. STATEMENT OF INTENT 6](#_Toc82182532)

[4. POLICY PRINICPLES 7](#_Toc82182533)

[5. DUTIES, ACCOUNTABILITIES AND RESPONSIBILITIES 12](#_Toc82182534)

[6. TRAINING AND GUIDANCE 17](#_Toc82182535)

[7. IG INCIDENT REPORTING AND MANAGEMENT 18](#_Toc82182536)

[8. DATA SECURITY AND PROTECTION TOOLKIT (DSPT) 18](#_Toc82182537)

[9. MONITORING COMPLIANCE WITH THIS DOCUMENT 19](#_Toc82182538)

[10. REFERENCES/BIBLIOGRAPHY 20](#_Toc82182539)

[11. RELATED PRACTICE POLICY/ PROCEDURE 21](#_Toc82182540)

[12. REVIEW 23](#_Toc82182541)

[13. APPENDIX 23](#_Toc82182542)

# SCOPE

This policy is applicable to all staff who are directly employed by and for whom **Greenbank Surgery** has a legal responsibility for, who will need access to personal, confidential and / or corporate information at the Practice. Further, this policy applies to all third parties and others authorised to undertake work on behalf of the Practice. The collective term ‘staff’ is used throughout this policy to mean all these groups.

# INTRODUCTION

This policy aims to set out the minimum policy standards and approach across the Practice for confidentiality, integrity and availability of information also known as Information Governance.

The Practice has an Information Governance (IG) framework in place (detailed within this policy) to help guide staff look after the information they need for their work, and ensure this information is protected on behalf of all service users, which includes patients and staff.

Information Governance is a framework that brings together all of the requirements, standards and best practice that apply to the handling of information, specifically information that contains personal confidential information, allowing:

* Implementation of central advice and guidance
* Compliance with the law
* Year on year improvement plans

It also provides a consistent way for staff to deal with the many different information handling requirements including:

* Information Governance Management
* Clinical Information assurance for Safe Patient Care
* Confidentiality and Data Protection assurance
* Corporate Information assurance
* Information Security assurance
* Secondary use assurance
* Respecting data subjects’ rights regarding the processing of their personal data

The framework provides a summary / overview of how the Practice is addressing the Information Governance agenda and how the Practice will fulfil their obligations when handling the personal confidential information its holds from whatever source that is not in the public domain.

The Practice has a duty to comply with data protection legislation such as the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), the Freedom of Information Act 2000 (FOIA 2000), and to meet Information Governance (IG) / Information Security / NHS specifications and requirements mainly relating to the National Data Guardians Data Security Standards and other related legislation, guidance and contractual responsibilities to support the assurance standards of the Data Security and Protection Toolkit (DSPT).

This formal mandatory framework known as the DPST that leaders of all health and social care organisations must commit to is set out in the National Data Guardian’s ten data security standards which is used to assess information governance performance and provide a benchmark.

It allows organisations to demonstrate their compliance with the legislation by evidencing the arrangements that have been put in place via embedded policies and procedures (refer to Section 8).

The Practice recognises the importance of reliable information, both in terms of clinical management of individual service users and the efficient management of services and resources. Information Governance plays a key part in supporting Clinical Governance, Service Planning and Performance Management.

# STATEMENT OF INTENT

The purpose of this policy is to inform all staff (permanent or otherwise), of their Information Governance responsibilities and the management arrangements and other policies that are in place to ensure demonstrable compliance. This is the central policy in a suite of policies that informs staff of:

* Maximising the value of organisational assets by ensuring that Practice demonstrates data is:
  + Held securely and confidentially
  + Processed fairly and lawfully
  + Recorded accurately and reliably
  + Used effectively and ethically; and

Shared and disclosed appropriately and lawfully

* Protecting the Practice’s information assets from all threats, whether internal or external, deliberate or accidental, to do this Practice will ensure:
* Information will be protected against unauthorised access
* Confidentiality of information will be assured
* Integrity of information will be maintained
* Information will be supported by the highest quality data
* Regulatory and legislative requirements will be met
* Business continuity plans will produced, maintained and tested
* Information governance and security training will be available to all staff, and
* All information governance breaches, actual or suspected, will be reported to, and investigated by, the Information Governance team in conjunction with the Data Protection Officer (DPO).

This policy covers all aspects of information within the Practice including (but not limited to):

* Service User information
* Personnel Information
* Organisational Information

This policy covers all aspects of handling information, including (but not limited to):

* Paper and electronic filing systems
* Communications, including those sent by post, electronic mail, text messaging
* Information that is stored in and/or processed by information systems including servers, personal computers (PCs), any other mobile device
* Information that is stored, copied, moved or transferred to any type of removable or portable transmission, both internal or externally to a third party.

The Practice recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The Practice fully supports the principles of corporate governance and recognises its public accountability but equally places importance on the confidentiality of, and the security arrangements to safeguard both personal confidential information about service users and staff and commercially sensitive information.

The Practice believes that accurate, timely and relevant information is essential to deliver the highest quality healthcare. As such, it is the responsibility of all Clinicians and Managers to ensure and promote the quality of information and to actively use information in decision making processes.

# POLICY PRINICPLES

The principles are to establish and maintain the security and confidentiality of information, specifically personal confidential information held in information systems, applications and networks owned or held by the Practice by ensuring:

* All members of staff are aware of their personal responsibilities and fully comply with the relevant legislation as described in this and other policies.
* The management and accountability arrangements for IG within the Practice are described.
* Confidentiality of information will be assured, recognising where it is appropriate to share whilst complying with the relevant legislation.
* Proactive use of information within the organisation and between other organisations both for patient care and service management as determined by law, statute, and best practice.
* Recognising the need to share personal confidential information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and, in some circumstances, the public interest.
* Information is protected against unauthorised access by introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibility and the need for an appropriate balance between openness and confidentiality in the management and use of information.
* Understanding that the integrity of information must be maintained, and information must be supported by the highest quality data in order to provide a high-quality service.
* Regulatory and legislative requirements will be met and where not informing and advising that penalties will be significantly increased for any infringement of the UK GDPR principles and data breaches
* Information governance and security training will be available to all staff creating a level of awareness which will be refreshed annually.
* The Practice complies with the requirements contained in the Data Security and Protection Toolkit, and,
* All information governance breaches, actual or suspected, will be reported to, and investigated by, the Practice Manager with support from Mid Mersey Digital Alliance Information Governance team in conjunction with the DPO and escalated to the Practice Senior Partners and Caldicott Guardian where necessary; and reported to the regulatory authority (the Information Commissioner’s Office, ICO) within 72 hours if assessed as high risk.

There are 4 key interlinked strands to the Information Governance Policy:

* Openness and Information Sharing
* Legal Compliance
* Information Security
* Information Quality Assurance

**4.1. Openness and Information Sharing**

* The Practice has an obligation as a Data Controller to notify the ICO of the purposes for which it processes personal data. Notification monitoring within the organisation is carried out by the Practice Manager with support from Mid Mersey Digital Alliance IG team and Practice DPO. Individual data subjects can obtain full details of the organisation’s data protection registration / notification with the ICO from their website: (www.ico.gov.uk).
* Non-confidential information about the Practice and its services will be available to the public through a variety of media, in compliance with the FOIA 2000 and EIR 2004. The organisation’s Publication Scheme will continue to meet the requirements of the ICO’s Model Scheme for health bodies.
* The Practice will ensure that the principles of Caldicott and the regulations outlined in the current Data Protection Legislation always underpin the management of personal confidential information.
* The organisation recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The Practice needs to share personal information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and, in some circumstances, the public interest. The Practice will ensure that when sharing it does so in accordance with the current Data Protection legislation.
* All service users, patients and staff should have ready access to information relating to themselves. Knowing their data rights as a patient and / or a member of staff. There are clear procedures and arrangements for handling requests for personal information from individuals detailed in the organisation’s Subject Access Request Procedure.
* The Practice will undertake or commission regular assessments and audits of its policies and arrangements for openness.

The Practice will publish a Privacy Notice consistent with the requirements of the Data Protection Act 2018, to provide individuals with information around the purposes for processing their personal data.

**4.2. Legal Compliance**

* Information Governance encompasses legal requirements, ethical considerations, national guidance and best practice in information handling, including:
  + Common Law Duty of Confidentiality
  + Human Right Act 1998
  + Data Protection Act 2018
  + UK General Data Protection Regulations 2018 (UK GDPR)
  + Freedom of Information Act 2000
  + Health and Social Care Act 2012
  + Information Quality Assurance
  + Records Management
  + Information Security
* The Practice processes personal confidential information about its employees, patients and other individuals for various purposes (for example, the effective provision of healthcare services). To comply with the current Data Protection legislation information must be ‘processed,’ collected and used fairly, stored safely and not disclosed to any unauthorised person. The current Data Protection legislation applies to both manual and electronically held data for living persons. The lawful and correct treatment of personal confidential information is key to maintaining confidence within the Practice and the individuals with whom it deals. The Practice will comply with the Data Protection Principles setting out the main responsibilities for organisations.
* The current Data Protection legislation and the common law duty of confidentiality should underpin the development of any information sharing decision. As data controllers, the Practice have a duty to comply with the Data Protection Principles (Article 5 of the UK GDPR):

a) processed lawfully, fairly and in a transparent manner in relation to individuals.

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the current Data Protection Legislation in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

* In accordance with Article 5 (a) the Practice will identify a lawful basis when processing personal confidential information, this includes the sharing of personal data.
* Patient and/or staff information will be shared with other agencies in accordance with agreed protocols and relevant legislation (e.g., Health and Social Care Act 2012, Crime and Disorder Act 1998, Protection of Children Act 1999) and the appropriate lawful basis for sharing will be identified.
* Where appropriate informed and explicit consent will be sought from the data subject and recorded, for the collection, processing and disclosure of data if this is deemed as the appropriate lawful basis.
* Individual will be informed of the purpose for which information is being collected / processed and who may access it. This will be via the Practice’s Privacy Notice (Article 5 (a)).
* The Practice will comply with the provisions of Article 12 - 22 of the UK GDPR and will establish and maintain appropriate and adequate administration arrangements for responding to individual right requests (e.g. Subject access) within the timescales defined under the Act. The Practice will undertake or commission an external assessment of its Information Governance Policies in line with the Data Security and Protection Toolkit annual review to check its compliance with legal requirements. The Practice will establish and maintain policies to ensure compliance with the common law duty of confidentiality and all relevant Acts of Parliament.

**4.3. Information Security**

* The Practice will establish, implement and maintain policies for the effective and secure management of its information assets and resources.
* Systems will be established to ensure that corporate records including health records are available and accessible at all times.
* Effective authorisation procedures for the use and access to personal confidential information and records, ensuring that there are strong access controls for all information systems in use at the Practice will be established.
* The Practice will ensure there are audit trails and monitoring of user activity built-in to information systems
* The Practice will ensure that all portable electronic media is encrypted
* The Practice will maintain an accurate and up-to-date information asset register.
* The Practice will ensure the secure disposal of data and hardware when disposal is required.
* The Practice will undertake or commission regular assessments and audits of its information and IT security arrangements as part of the Data Security and Protection Toolkit annual review.
* The Practice will promote effective confidentiality and security practice to its staff through policies, procedures and training. These policies and procedures are available on the Practice Internet and from the Information Governance team.
* The Practice will undertake Data Protection Impact Assessments, Supplier’s Due Diligence to determine appropriate security controls are in place for existing or potential information systems.
* The Practice will establish and maintain incident reporting procedures which will include the monitoring and investigation where appropriate, of reported instances of actual or potential breaches of confidentiality or information security.

**4.4. Information Quality Assurance**

* The Practice will establish and maintain policies and procedures for information quality assurance and the effective management of records.
* The Practice will promote records management through policies, procedures and training.
* The Practice will undertake or commission regular assessments and audits of its information quality and records management arrangements.
* Information Asset Owners and Line Managers are expected to take ownership of, and seek to improve, the quality of information within their services.
* Wherever possible, information quality should 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.
* Quality control in record conversion is extremely important to the Practice. Where information is scanned there is the potential for loss of some of the information. In all cases, the organisation will review the information loss and make a decision as to whether the loss is acceptable
* The Practice will refer to the current Records Management Code of Practice for Health and Social Care as its standard for records management.

# 5. DUTIES, ACCOUNTABILITIES AND RESPONSIBILITIES

**The Senior Partners**

The Senior Partners have the overall responsibility for the strategic and operational management of the Practice including and ensuring that Practice policies comply with all legal, statutory and good practice guidance requirements.

**Practice Manager**

The Practice/Office Manager provides advice to the Practice Senior Partners in regard to any information risk and will assure the Practice Management that IG and information security risks are being managed effectively.

The Practice/Office Manager will review and submit the Data Security and Protection Toolkit Self-Assessment annually and provide relevant assurances to the Practice Management staff

**Caldicott Guardian**

The Caldicott Guardian is responsible for ensuring that the Practice processes satisfy the highest practical standards for handling patient information.

The role of the guardian is to safeguard and govern uses made of patient information within the Practice, as well as data flows to other NHS and non-NHS organisations. Caldicott Guardianship is a key component of broader Information Governance.

The Guardian is responsible for the establishment of procedures governing access to, and the use of, person-identifiable patient information and, where appropriate, the transfer of that information to other bodies.

The Guardian utilises the UK Caldicott Guardian Council’s [‘A Manual for Caldicott](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/581213/cgmanual.pdf) Guardians’ to assist them in embedding the Caldicott principles within the Practice. This document sets the role of the Caldicott Guardian within an organisational Caldicott / Confidentiality function which is itself a part of broader Information Governance.

Both the Caldicott Guardian and the Practice Manager will be assisted in their work by a comprehensive support structure.

The Practice also has a named Deputy Caldicott Guardian who is available to act as deputy for the Caldicott Guardian when they are not available.

**Data Protection Officer**

The General Data Protection Regulation (GDPR) requires that all public authorities nominate a Data Protection Officer (DPO). Section 7 of the Data Protection Act 2018 defines the Practice as a public authority and as such must nominate a DPO.

The DPO role is a senior role with reporting channels directly to the highest level of management and has the requisite professional qualities and expert knowledge of data protection compliance.

Article 39 of the GDPR defines the duties of the DPO as:

• Informing and advising employees about their obligations to comply with the GDPR, the Data Protection Act and other legislation and monitoring compliance with such legislation.

• Monitoring compliance with data protection policies and appropriate documentation that demonstrates commitments to and ownership of IG responsibilities, for example, production of an IG Framework document supported by relevant policies and procedures.

• Raising awareness of data protection issues with staff and at a senior level

• Raising awareness of data security training and monitoring compliance.

• Providing advice and guidance on Data Protection Impact Assessments (DPIA’s) as per Article 38 of the GDPR.

• To be the first point of contact with the supervisory authorities, including the ICO, and individual whose data is being processed.

• Developing and maintaining comprehensive and appropriate documentation

• Monitoring compliance and carrying out Audits

• Maintaining expert knowledge in data protection.

The DPO for Practice is - Mid Mersey Digital Alliance

**Information Asset Owner**

IAOs under the responsibility of the Practice Manager will:

* Lead and foster a culture that values, protects and uses information for the success of the Practice and benefit of its patients and staff.
* Know what information comprises or is associated with the asset(s) and understand the nature and justification of information flows to and from the asset.
* Know who has access to the asset, whether system or information, and why, and ensure access is monitored and compliant with policy.
* Understand and address risks to the asset and provide assurance to the Practice Manager and Senior Partners
* Ensure there is a legal basis for processing and for any disclosures.
* Ensure all information assets are recorded on the Information Asset Register (IAR) and maintained.
* Refer queries about any of the above to the Data Protection Officer and Information Governance team, and
* Undertake specialist information asset training as required.

**Information Asset Administrators**

The IAO can assign day to day responsibility for each Information Asset to an IAA or other manager.

**Mid Mersey Digital Alliance Information Governance Team**

The Information Governance Team is responsible for advising on strategic direction, the development of policy and guidance for the Practice, and also operational support to the Practice on Information Governance compliance.

Key tasks include:

* Developing and maintaining comprehensive and appropriate documentation that demonstrates commitments to and ownership of IG responsibilities, for example, production of a data security (IG) framework document supported by relevant policies, procedures and guidance.
* To ensure that there is top level awareness and IG support to the Practice.
* Ensuring that annual DSPT assessments and regular improvement plans / progress reports are prepared.
* Ensuring that the approach to information handling is communicated to the Practice

Providing a focal point for the resolution and / or discussion of data security / information governance issues.

**Staff and workers**

All staff and workers are responsible for ensuring they are aware of the Information Governance requirements and ensuring they comply with these on a day-to-day basis.

Staff will receive instruction and direction regarding the policy from several sources:

* Practice Manager
* DPO
* Mid Mersey Digital Alliance Information Governance team
* Policy / strategy and procedure manuals
* Line manager
* Specific training course
* Other communication methods, for example, team meetings; and
* Practice website

All staff are mandated to undertake mandatory information governance training in line with the Practice training needs analysis.

All staff must make sure that they use the Practice IT systems appropriately and adhere to the Acceptable Use Policy.

Section 170 (1) of the Data Protection Act 2018: Unlawful obtaining etc of personal data, states it is an offence for a person knowingly or recklessly:

(a) to obtain or disclose personal data without the consent of the controller;

(b) to procure the disclosure of personal data to another person without the consent of the controller, or

(c) after obtaining personal data, to retain it without the consent of the person who was the controller in relation to the personal data when it was obtained.

Staff must report any incident involving a breach or suspected breach of the Data Protection legislation to their line manager immediately and via the Practice Incident Reporting System.

# 6. TRAINING AND GUIDANCE

The Practice recognises that to gain the commitment of staff and workers to support and meet local information governance and security requirements they must be aware of, and understand why various procedures are in place.

* IG Training detailing the handling of personal confidential information will be provided

The National Data Guardian Standard 3 states that “All staff complete appropriate annual data security training and pass a mandatory test.” This is included in the Data Security and Protection Toolkit (assertion 3.3.1) which the Practice must comply with and have a target of 95% compliance every year.

The IG team has developed appropriate training based on the “Data Security Awareness**”** module by NHS Digital. The training module is accessible online via the Practices E-Learning programme or delivered face to face. All Practice staff (including temporary / agency) must complete and pass this module.

The Practice will ensure that all staff and workers are provided with the necessary security guidance, awareness and appropriate training to discharge their data protection and information security responsibilities. Those staff who have additional responsibilities within their role may be required to undertake appropriate additional modules as identified in the Information Governance Training Needs Analysis (TNA).

All staff and workers will be made aware of the contents and implications of this Information Governance and (where appropriate) information security procedures as irresponsible or improper actions by users may result in disciplinary action(s).

# 7. IG INCIDENT REPORTING AND MANAGEMENT

All data breaches / IG incidents concerning personal confidential data must be reported via the Practice’s Incident Management Procedure and escalated if and when required. The Data Security and Protection Breaches / Incident Reporting Policy and Procedure will inform staff of the extra reporting requirements and provide further information on the process and next steps.

A breach is defined in Article 4(12) of the UK GDPR as a “Personal data breach” this means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

IG are consulted regarding all data breaches and co-ordinate the investigation / scoring of the incident and where necessary this is escalated to the DPO, SIRO and or the Caldicott Guardian.

The scoring of the data breach is based on Article 33 of the GDPR ‘risk to the rights and freedoms of individuals. NHS Digital guidance called “The Guide for Notification of Data Security and Protection Incidents Guidance” is used to ascertain the score of the incident as per the link: https://www.dsptoolkit.nhs.uk/Help/29

The Practice Manager will seek guidance from MMDA IG team and their DPO if the data breach is scored high and may need to be reported to the ICO. If this concerns patient data, the IG Team will also seek the advice from the Caldicott Guardian. Before any data breaches are reported to the ICO the DPO will review such incidents and make recommendation to the Practice.

# 8. DATA SECURITY AND PROTECTION TOOLKIT (DSPT)

The DSPT is a mandatory performance self-assessment tool that enables organisations to measure and publish their performance against the National Data Guardian’s ten data security standards, and the associated NHS Digital CareCERT suite of services across three leadership obligations:

* People – ensure staff are equipped to handle information respectfully and safely, according to the Caldicott Principles
* Process – ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses
* Technology – ensure technology is secure and up-to-date

The requirements of the Data Security and Protection Toolkit (DSPT) are designed to encompass the National Data Guardian review’s 10 data security standards which are:

* Personal Confidential Data.
* Staff Responsibilities.
* Training.
* Managing Data Access.
* Process Reviews.
* Responding to Incidents.
* Continuity Planning.
* Unsupported Systems.
* IT Protection.
* Accountable Suppliers.

The requirements of the DSPT also support key requirements under the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018. This is an annual work programme which is a requirement for all NHS organisations with an online submission at the end of the June.

The Practice has a well embedded information governance framework and governance process in place to ensure compliance with the annual DSPT.

# 9. MONITORING COMPLIANCE WITH THIS DOCUMENT

The Practice will conduct year-on-year assessments and develop improvement plans by:

* Monitoring its compliance with Information Governance Framework by completing a yearly assessment and attaining standard met within the DSPT.

The table below outlines the Practices’ Key Performance indicators and monitoring arrangements for this Strategy. The Practice reserves the right to commission additional work or change the monitoring arrangements to meet organisational needs.

**Key Performance Indicators of this Policy**

|  |  |  |
| --- | --- | --- |
| **Describe Key Performance Indicators (KPIs)** | **Frequency of Review** | **Lead** |
| Duties are carried out as described in the Policy | Annually | Practice/Office Manager |
| Compliance will be monitored via the DSPT | Annually | Practice/Office Manger |
| Information Governance Training | Training will be monitored in line with the Practice Policy. | Practice/Office Manager |

# 10. REFERENCES/BIBLIOGRAPHY

Legal Acts:

* UK General Data Protection Regulation
* Data Protection Act 2018
* Freedom of Information Act 2000
* Environmental Information Regulations
* Access to Health Records Act 1990
* Regulation of Investigatory Powers Act
* Health and Social Care Act 2012
* Human Rights Act 1998.

Supporting Documents:

* NHS Code of Confidentiality
* Caldicott Guardian Manual 2017
* NHS Information Risk Management.
* Records Management NHS Code of Practice
* Data Security and Protection Toolkit (DSPT)
* Caldicott Reports
* ICO Guidance

# 11. RELATED PRACTICE POLICY/ PROCEDURE

The Practice will maintain this Information Governance Policy Framework. This will be supported by a set of related information governance policies and procedures which are aligned with the NHS Operating Framework and the Data Protection and Security Toolkit requirements.

Associated Information Governance Policies:

|  |  |
| --- | --- |
| **Policies** | **Description** |
| Confidentiality Code of Conduct Policy | This document is a guide to required practice and responsibility for those who work within or under contract to the Practice concerning confidentiality of staff and patient information |
| Data Security and Protection Breaches / Incident Reporting Policy and Procedure | This document is to inform all staff of the process for reporting personal data breaches and the process that the Practice’s employees must follow |
| Corporate Records Management Policy | The intention of the document is to outline a health records policy for the Practice, that will ensure that the organisation is in a position to fulfil its statutory responsibilities in the delivery of quality care services throughout the Practice, whilst maintaining accountability arrangements to all key stakeholders |
| Freedom of Information Act Policy | This Freedom of Information Policy is a statement of the way that the Practice will ensure compliance with the Act. It is not a statement of how compliance will be achieved; this will be a matter for operational procedures. This Policy will provide a framework within which the Practice will ensure compliance with the requirements of the Act and will underpin any operational procedures and activities connected with the implementation of the Act |
| Data Quality Policy | This document reinforces the Practice’s commitment to data quality. The Policy is intended to cover all data that is entered onto computerised systems within the Practice. It primarily covers data relating to patients and the delivery and recording of their care, but can also include other data that relates to financial management, service management performance and information governance |
| Registration Authority Policy | To ensure that the security and confidentiality of all Smartcard controlled systems is paramount and the Practice must conform to stringent national access procedures. It is also of importance that patients of the NHS are confident that their health records are being kept secure and confidential in line with the Summary Care Records Guarantee |
| Network Security Policy | This Policy governs use of the wired and wireless networks within the Practice. It governs remote access and arrangements where network resources and infrastructure provide staff with the ability to perform work-related duties from non-Practice sites. It defines the rules for network access for Practice owned and non-Practice owned devices as well as other NHS devices |
| Back up Policy | This policy defines the Practice approach to protection of data via backup |
| Mobile Device Policy | This policy sets out the criteria for issue of Practice provided mobile devices and devices that utilize the wireless network Service, the rules around their use, use of personal devices by staff, and acceptable use of Mobile devices on Practice premises by patients/visitors. |
| Remote Access Policy | Compliance with the Remote Access Policy will ensure the integrity and privacy of the Practice’s data and information systems for staff and providers who access systems remotely |

# 12. REVIEW

This policy will be monitored through staff awareness and supporting

evidence to the Data Security and Protection Toolkit.

This Policy will be reviewed in line with the review date documented above, and in accordance with the following, on an as and when required basis:

* Legislative changes
* Good practice guidance
* Case law
* Significant incidents reported, new vulnerabilities, and
* Changes to organisational infrastructure