

Suffolk GP Practice DPO Cluster

Information Governance Policy

| Policy Title / Reference | Author | Owner |
|-------------------------------|-----------------------------------|------------------|
| Information Governance Policy | Emma Cooper, Cluster DPO (Kafico) | Practice Manager |

| Version | Revision author | Version comments |
|---------|-------------------------------|--|
| 1 | Emma Cooper, Kafico Ltd (DPO) | Jan 18 New Draft |
| 1.1 | Emma Cooper, Kafico Ltd (DPO) | Jan 19 Jan 2019 Replaced 1998 DPA with 2018 Act. Replaced GDPR with "data protection legislation". |
| 1.1 | Emma Cooper, Kafico Ltd (DPO) | Jan 20 – Annual Review. No changes. |

1. Contents

| | |
|---|---|
| 2. Scope | 2 |
| 3. Introduction | 2 |
| 4. Statutory Mandatory Framework | 3 |
| 5. Accountable Parties | 4 |
| The Board | 4 |
| Senior Information Risk Owner (SIRO) | 4 |
| Information Asset Owners (IAOs) | 4 |
| Caldicott Guardian Function | 4 |
| Data Protection Officer (DPO) | 5 |
| All Staff | 5 |
| 6. Openness | 5 |
| 7. Privacy and Information Rights | 6 |
| 8. Information Security | 6 |
| 9. Information Quality and Records Management | 6 |
| 10. Associated Protocols | 7 |
| 11. Audit Schedule | 7 |

Suffolk GP Practice DPO Cluster

12. Review 8

2. Scope

This policy has been drafted for use by customers of Kafico Ltd across Norfolk and Waveney.

At the time of writing and unless alternative policies have been adopted locally, the policy applies to;

| | | |
|----------------------------------|-------------------------------|--|
| Acle Medical Partnership | Boughton Doctors Surgery | Hellesdon Medical Practice |
| Beccles Medical Centre | Bridge Street Surgery | Holt Medical Practice |
| Birchwood Surgery | Cromer Group Practice | Feltwell Surgery |
| Blofield Surgery | St Clement's Surgery | Great Massingham and Docking Surgeries |
| The Brundall Medical Centre | Castle Partnership | The Harleston Medical Practice |
| Coltishall Medical Practice | The Burnhams Surgery | Heacham Group Practice |
| Campingland Surgery | Drayton Surgery | St John's Surgery |
| Hoveton & Wroxham Medical Centre | Roundwell Medical Centre | Staithe Surgery |
| Ludham Surgery | Paston Surgery | Thorpewood Surgery |
| The Market Surgery | Prospect Medical Practice | Upwell Health Centre and Welle Ltd |
| Howdale Surgery | Sheringham Medical Practice | Watlington Medical Centre |
| Litcham Health Centre | Southgate and Wootton's | Wells Health Centre |
| Mundesley Medical Centre | St James Medical Practice | St Stephen's Gate |
| Manor Farm Medical Centre | The Fakenham Medical Practice | Plowright Medical Centre |
| Grimston Medical Centre | Aldborough Surgery | Bacon Road / Taverham |
| The Burnham Surgery | Reepham & Alysham Surgery | Lakenham Surgery |
| Oak Street Medical Practice | UEA Medical Centre | Woodcock Road Surgery |
| Old Catton Medical Practice | | |

3. Introduction

Information Governance (IG) is a set of multi-disciplinary structures, policies, procedures, processes and controls implemented to manage information at an organisational level.

Suffolk GP Practice DPO Cluster

Information Governance supports **The Practice's** immediate and future regulatory, legal, risk, environmental and operational requirements.

Information is a vital asset, both in terms of the commercial development and the efficient management of services and resources. It plays a key part in governance, service planning and performance management.

It is therefore of critical importance to ensure that information is appropriately managed, and that policies, procedures and management accountability and structures provide a robust governance framework for information management.

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 clinical and corporate governance and recognises the power of public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients, the public and staff and commercially sensitive information. **The Practice** also recognises the need to share information with commissioners, partners and other third parties in a controlled manner consistent with the established lawful basis.

This overarching Information Governance Policy and the associated protocols sets out **The Practice's** policy with respect to the governance of;

- Privacy
- Information and Cyber Security
- Data Quality and Records Management

4. Statutory Mandatory Framework

This policy serves to support **The Practice** to navigate and comply with the complex framework within which Information Governance operates.

This framework includes but is not limited to;

- NHS Act 2006
- Health and Social Care Act 2012
- Data Protection Act 2018
- Human Rights Act 1998
- Common Law Duty of Confidence

Suffolk GP Practice DPO Cluster

- Computer Misuse Act 1990
- General Data Protection Regulations (EU) 2016/679
- Mental Health Capacity Act 2005
- Children Act 1989
- DH Records Management Code of Practice
- DH Information Security Code of Practice
- DH Confidentiality Code of Practice

5. Accountable Parties

The Board

The Board has overall responsibility for Information Governance at **The Practice**. As the senior accountable officer, he/she is responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to provide the necessary assurance to internal and external stakeholders.

The Board has a particular responsibility for ensuring that **The Practice** meets its corporate legal responsibilities, and for the adoption of internal and external governance requirements.

Senior Information Risk Owner (SIRO)

The SIRO;

- leads and fosters a culture that values, protects and uses information for the success of the organisation and benefit of its customers.
- owns the organisation's overall information risk policy and risk assessment processes and ensuring they are implemented consistently by Information Asset Owners / Administrators.
- Owns the organisation's information incident management framework

Information Asset Owners (IAOs)

The IAO will;

Hold local responsibility for information risk management, devolved to the relevant directors, department leads by the SIRO. Business function leads within **The Practice** have overall responsibility for the management of risks generated by their information assets and are supported on a daily basis by Information Asset Administrators.

Caldicott Guardian Function

The Caldicott Guardian will;

Suffolk GP Practice DPO Cluster

- Produce procedures, guidelines and protocols to support staff in the appropriate management of patient information
- Provide a point of escalation and specialist advice for staff with respect to information sharing, acting as the conscience of the organisation
- bring to the attention of the relevant manager any occasion where the appropriate procedures, guidelines and protocols may have not been followed and raise concerns about any inappropriate uses made of patient information where necessary.

Data Protection Officer (DPO)

The DPO Will;

- inform and advise the organisation and its employees about their obligations to comply with the data protection legislation.
- monitor compliance with the data protection legislation, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, patients etc).

All Staff

All staff, whether clinical or administrative, who create, receive and use data have information governance responsibilities. Employees have a contractual and legal obligation to read and comply with all company policies and to attend mandatory training to support the appropriate management of information.

6. Openness

Non-confidential information related to **The Practice** and its services will be available to the public through a variety of media, in line with **The Practice's** overall commitment to transparency

The Practice will adopt and maintain clear procedures and arrangements for liaison with the press and broadcasting media

The Practice will adopt and maintain an Information Rights and Access Protocol and a Freedom of Information Protocol to provide guidance for handling queries from data subjects and the public.

Suffolk GP Practice DPO Cluster

7. Privacy and Information Rights

The Practice is committed to the privacy of its patients, staff and the public. **The Practice** will undertake or commission annual assessments and audits of its compliance with privacy legislation and will adopt and maintain protocol for completion of Data Protection Impact Assessments.

The Practice regards all Personal Data relating to staff as confidential except where national policy on accountability and openness requires otherwise

The Practice will adopt and maintain protocols to ensure compliance with the Data Protection Act, General Data Protection Regulations, Human Rights Act and the common-law confidentiality

The Practice will establish and maintain protocols for the controlled and appropriate sharing of personal information with other agencies, taking account of relevant legislation (e.g. Data Protection Act, Human Rights Act).

The Practice will ensure that contractual or best practice documents are in place for routine sharing of information between sharing partners.

8. Information Security

The Practice will adopt and maintain protocols for the effective and secure management of its information assets and resources

The Practice will undertake or commission annual assessments and audits of its information and IT security arrangements

The Practice will promote effective information and cyber security practice to its staff through policies, procedures and training

The Practice will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of information and cyber security

9. Information Quality and Records Management

The Practice will establish and maintain protocols and procedures for information quality assurance and the effective management of records

The Practice will undertake or commission annual assessments and audits of its information quality and records management arrangements

Suffolk GP Practice DPO Cluster

Managers will be expected to take ownership of, and seek to improve, the quality of information within their services

Wherever possible, information quality will 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.

The Practice will promote information quality and effective records management through protocols, procedures/user manuals and training

10. Associated Protocols

This policy should be read in conjunction with;

- Risk Management Policy
- Change Management Policy
- Information Rights and Access Protocol
- Information Sharing and Privacy Protocol
- Information Lifecycle and Data Quality Protocol
- Information / Cyber Security Protocol
- Information Incident Protocol
- Information Risk and Audit Protocol
- Data Protection Impact Assessment Protocol
- Freedom of Information Protocol

11. Audit Schedule

Compliance with this policy will be audited and the results fed into the Plan, Do, Check, Act Cycle described in the Information Risk and Audit Protocol.

| Policy Section | Compliance Evidence | Monitoring Method | Frequency |
|----------------------------------|---|-----------------------|-----------|
| 4 Accountable Parties | The most senior members of the organisation are regularly appraised of internal and external governance status and requirements including resource requirements | IG Audit | Quarterly |
| 4 Data Protection Officer | Changes within the organisation are subject to a Data Protection Impact Assessment | IG Audit | Quarterly |
| 4 Data | The DPO is being made aware of all | Processing Activities | Quarterly |

Suffolk GP Practice DPO Cluster

| | | | |
|---|---|----------|-----------|
| Protection Officer | processing activities across the organisation | Log | |
| 6 Privacy and Information Rights | The organisation has an effective infrastructure in place to ensure privacy and to give effect to the information rights of individuals | IG Audit | Quarterly |
| 7 Information Security | The organisation has an effective infrastructure in place to ensure information security | IG Audit | Quarterly |
| 8 Information Quality and Records Management | The organisation has an effective infrastructure in place to ensure information security | IG Audit | |

12. Review

This policy will be reviewed every two years or sooner where necessary.