Information Risk and Audit Protocol

|  |  |  |
| --- | --- | --- |
| Policy Title / Reference | Author | Owner |
| Information Risk and Audit Protocol | 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 2019 Replaced 1998 DPA with 2018 Act. Replaced GDPR with “data protection legislation”.Added new twice-yearly compliance audit. |
| 1.1 | Emma Cooper, Kafico Ltd - DPO | Jan / Feb 20 – Annual review – no amendments |

Contents

[2. Scope 2](#_Toc6745740)

[3. Definitions 3](#_Toc6745741)

[4. Introduction 3](#_Toc6745742)

[5. Statutory Mandatory Framework 3](#_Toc6745743)

[6. Accountable Parties 4](#_Toc6745744)

[7. Risk Management Cycle 4](#_Toc6745745)

[8. Audit Completion and Reporting 5](#_Toc6745746)

[9. Information Incidents 5](#_Toc6745747)

[10. Associated Protocols 5](#_Toc6745748)

[11. Audit Schedule 6](#_Toc6745749)

[12. Review 6](#_Toc6745750)

[Appendix A: Twice Yearly Data Security Audit 7](#_Toc6745751)

# Scope

This protocol has been drafted for use by customers of Kafico Ltd across Suffolk.

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

|  |  |  |
| --- | --- | --- |
| Barrack Lane | Martlesham | Mendlesham |
| Burlington Road | Ravenswood | Wickhambrook |
| Framlingham | Stanton (west) | Church Farm Surgery (Aldeburgh) |
| Botesdale Health Centre | The Birches | Framfield |
| Felixstowe Road | Mount Farm | Saxmundham |
| Hawthorn Drive | Swan and Forest | Guildhall & Barrow |
| The Surgery, Leiston | Glemsford | Peninsula |
| Victoria Surgery | Lakenheath | Little St John Street |
| Ivry Street | Ixworth | Grove Medical Centre |
| Guildhall and Barrow |  |  |

# Definitions

**Personal Confidential Information** This term is intended to cover information captured by the Data Protection Act 2018 / GDPR (identifiable information about the living), information covered by the Common Law Duty of Confidence / Tort of Misuse of Private Information and finally, information covered by Article 8 European Convention for Human Rights.

# Introduction

This protocol intends to support **Practice** staff in managing information risk to protect the organisation and its stakeholders from the inherent risks associated with processing Personal Confidential Information as well as protecting The **Practice**’s corporate memory and information as a valuable asset.

# Statutory Mandatory Framework

Information Risk Management is a discipline that supports The **Practice’s** ability to operate within a complex framework of privacy legislation including Data Protection legislation, Common Law Duty of Confidence, Article 8 European Convention of Human Rights, Computer Misuse Act 1990 as well as health specific mandatory codes. Effective Information Risk Management protects the organisation and its stakeholders and allows for effective risk mitigation, planning and allocation of resources.

# Accountable Parties

See Information Governance Policy for key roles.

All staff, whether management or administrative, who create, receive and use Personal Confidential Information have responsibilities to ensure effective reporting and management of information risk for The **Practice**. 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.

# Risk Management Cycle

The **Practice**’s Information Risk Management takes the form of a Plan, Do, Check, Act cycle as demonstrated in the diagram below.



All audit, review and incident outcomes are fed into senior management where recommendations are made as to how controls can be applied or improved for greater assurance.

This Protocol sits beneath the **Practice’s** Risk Management Policy.

# Audit Completion and Reporting

**The Practice** risk register must include risks inherent to the processing of Personal Confidential Information

The Information Risk must be reviewed Quarterly and escalations made to the SIRO or Data Protection Officer

The DPO must assess the residual risk from any Data Protection Impact Assessments and information incidents

The Information Governance Audit must be completed annually

Processors must be monitored for compliance with service contracts in relation to privacy and data security

# Information Incidents

Any suspected or actual incidents involving Personal Confidential Information must be reported immediately in line with the Information Incident Protocol.

# Associated Protocols

This policy should be read in conjunction with the following, where present;

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

# Audit Schedule

Information Risk will be audited through the Information Governance Audit at Appendix A.

# Review

This protocol will be reviewed every year or sooner where necessary

# Appendix A: Twice Yearly Data Security Audit

|  |  |
| --- | --- |
| Suggested Exploration | Notes |
| Are you and your colleagues aware of the location of the policies and protocols related to data protection and security provided by your DPO? |   |
| Are you and your team referring any information requests to your DPO for support when required? This would include - data amendment, deletion, restriction, objections to process and requests for copies of records. |   |
| Will there be any new or changed processes introduced in the next three months or have there been since last audit? |   |
| Will there be any new or changed sharing partners (other organisations that we send personal data to or receive from) in the next three months or have there been any since last return? |   |
| Is your practice undertaking any processes involving personal data that are not listed here?

|  |  |  |
| --- | --- | --- |
| *REFERRALS* | *INFORMATION RIGHTS REQUEST* | *PATIENT TEXTS* |
| *TEST RESULTS* | *MEDICAL REPORTS REQUEST* | *PATHOLOGY COURIER* |
| *DISCHARGE NOTICES* | *CONFIDENTIAL WASTE DESTRUCTION* | *CORONER REPORTS* |
| *GP+* | *DIGITAL DICTATION* | *OUT OF HOURS (OOH)* |
| *EPS* | *PATIENT ACCESS* | *HOME VISITS* |
| *RESEARCH* | *INCIDENT MANAGEMENT* | *REMOTE WORKING* |
| *PATIENT 500* | *Improved Access* | *GP Connect* |
| *AMP Sexual Health Services* | *Referral to Social Prescribing* | *Enhanced Care to Care Homes* |
| *COMMISSIONER REPORTS* | *SELF CHECK IN SCREENS* | *TELEPHONE RECORDING* |
| *INVOICING FOR PATIENT NOTES / COPY RECORDS* | *COMPLAINTS / PALS* | *DIABETIC EYE SCREENING* |

 |   |
| Are all of the third-party providers that process personal data (this includes de-identified data) (for example CCTV provider, confidential waste providers, IT and software providers) listed here?*please add any new ones*

|  |  |  |  |
| --- | --- | --- | --- |
| *Avena* | *ISS pathology Couriers* | *Health Intelligence* | *UK Mail / iMail* |
| *Restore* | *NE Essex, Suffolk Path Service* | *Child Health Provide* | *Mysurgery Website* |
| *Shred Station* | *The Pathology Partnership* | *Eclipse Solutions (Safety Reports)* | *Numed* |
| *Shred-It* | *ERS Medical* | *MJOG* | *Northwest Ostomy Supplies* |
| *Onsite Shredding* | *City Sprint*  | *Sentinel 24hr ECG*  | *CCTV* |
| *Citrus* | *Capita* | *Cardio Vision 24hr BP* | *Dragon Security* |
| *Bolton Brothers* | *Norfolk Copiers Ltd* | *WebAdore* | *STC Solutions* |
| *BIFFA* | *Copy IT* | *Docmail* | *Dionysys Ltd* |
| *PHS* | *APR Telecomms / Tollring* | *NHS Choices* | *ECS computers* |
| *Lexacom 3* | *ScanAll pro* | *Fairways* | *Larkin Gowen Accountants* |
| *Crescendo* | *Scan & Collate* | *IRIS accounting software* | *Xero* |
| *Olympus*  | *DCA Photocopiers* | *MB* | *National Pharmacy Association* |
| *iGPR* | *PayeDoc* | *Sage* | *AGEM - Medicines Optimisation* |
| *Medical Defence Union* | *Systm One (TPP)* | *Cellmark (Cellmark as Controller, Practice as Processor)* | *EMIS Web* |

 |   |
| Has your practice completed a clinical system access audit within the last 12 weeks? |   |
| How do you currently ensure that you are not retaining records for longer than their intended use? Do you regularly destroy records in line with their retention schedules? |   |
| Apart from your main clinical system, what systems hold personal data (this includes employee data)? |   |
| Do these systems have Role Based Access (the privileges that people have are linked to their position within the practice)  |   |
| Is your current file structure logical and up to date? |   |
| Do you have any difficulties locating records or with duplications? |   |
| Can you confirm that all records pertaining to the practice’s activities are located in the shared drive and not on personal / individual drives? |   |
| Do you have any concerns about data security that we should be aware of? |  |
| Do your employee contracts have confidentiality clauses? |  |
| Have all you staff been trained in Information Governance within the last 12 months? |  |
| Do all staff wear ID badges? |   |
| Is reception staffed during opening hours? |   |
| Are non-public entry points secured by key pads or locked? |   |
| Do all visitors sign in? |   |
| Do you have [THESE](https://www.kafico.co.uk/copy-of-transparency-privacy-notice-1) posters in visible positions within your working premises?  |  |