Information / Cyber Security Protocol

|  |  |  |
| --- | --- | --- |
| Policy Title / Reference | Author | Owner |
| Information / Cyber Security Protocol | Emma Cooper, Cluster DPO (Kafico) | Senior Information Risk Owner |

|  |  |  |
| --- | --- | --- |
| Version | Revision author | Version comments |
| 1 | Emma Cooper, Kafico Ltd, DPO | New Draft |
| 1.1 | Emma Cooper, Kafico Ltd, DPO | Jan 2019 Replaced 1998 DPA with 2018 Act. Replaced GDPR with “data protection legislation”. |
| 1.1 | Emma Cooper, Kafico Ltd, DPO | Jan / Feb 20 – Annual review – no amendments |

Contents

[2. Scope 2](#_Toc6743703)

[3. Definitions 3](#_Toc6743704)

[4. Introduction 4](#_Toc6743705)

[5. Statutory Mandatory Framework 4](#_Toc6743706)

[6. Accountable Parties 4](#_Toc6743707)

[7. Introduction 4](#_Toc6743708)

[8. Identity, Authentication and Authorisation 5](#_Toc6743709)

[9. Accountability, Audit and Compliance 5](#_Toc6743710)

[10. Information Risk 5](#_Toc6743711)

[11. Technical Controls 6](#_Toc6743712)

[12. Procedural Controls 7](#_Toc6743713)

[13. Information Incidents 7](#_Toc6743714)

[14. Associated Protocols 7](#_Toc6743715)

[15. Audit Schedule 8](#_Toc6743716)

[16. Review 8](#_Toc6743717)

[Appendix A User Authorisation Process 9](#_Toc6743718)

# 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 to discharge their duties in a way that supports effective information security and protect **The Practice** from cyber threats and identify vulnerabilities.

# Statutory Mandatory Framework

Data Protection legislation mandates the implementation of appropriate organisational and technical measures to ensure the confidentiality, availability and integrity of **The Practice**’s information assets from unauthorised access, loss, theft or from cyber threats and vulnerabilities. The protocol has been developed with reference to Cyber Essentials and the Data Security and Protection Toolkit.

# 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 security for **The Practice**. Employees have a contractual and legal obligation to read and comply with all policies and to attend mandatory training to support the appropriate management of information.

# Introduction

Information security is made up of three major concepts;

* Confidentiality: information will only be available to a limited number of individuals
* Integrity: information is useful, complete and accurate and remains so.
* Availability: that information is available when and as required[[1]](#footnote-1).

Without high-standards of information security, supported by systematic processes and practice, we cannot realise these concepts within **The Practice**.

# Identity, Authentication and Authorisation

Default passwords (factory settings) on all equipment must be amended including Computers, Internet Routers and mobile devices.

System Administrator access to systems must be provided only to nominated, limited individuals and those accounts must also be subject to audit.

Users must change their passwords periodically and the password must meet a pre-defined threshold.

Passwords must not be shared or written down.

Password changes must be authorised via the User Authorisation Process at Appendix A.

Authorisation of users must be in line with the User Authorisation Process at Appendix A.

Role Based Access Controls must be implemented to ensure that access is limited to the correct individuals and the correct information assets.

# Accountability, Audit and Compliance

Information Assets Owners must be allocated for all key information assets and are responsible for monitoring risk, alerting the SIRO to changes or issues and overseeing the information security for the asset in question.

All information systems must have the facility to record changes made to data, monitor access to the system and report on data quality.

All information systems must have the facility to produce audit, such that such audits can identify inappropriate use or activity.

# Information Risk

Reports must be produced quarterly that identify threats to and vulnerabilities of the confidentiality, availability and integrity of the organisations information assets.

The impact of the threats must be considered at the appropriate **practice** meeting and appropriate physical, technical and organisational controls applied.

Information Security risks must be fed into the practice’s Information Risk Management Programme and aligned with the Plan, Do, Check, Act process identified in the Information Risk and Audit Protocol.

# Technical Controls

Only **Practice** issued encrypted media should be used by staff including CD, DVD, USB, mobile phones and computers.

Reports must be produced quarterly that identify performance and activity of firewalls and other malware countermeasures that protect the confidentiality, availability and integrity of the organisations information assets.

The impact of the threats must be considered at the Information Governance Steering Group and appropriate physical, technical and organisational controls applied.

Firewalls must be activated on all **Practice** computers and devices that connect to the internet

Default settings for firewalls must be changed on all computers, devices and routers

Software applications that are not used, must be removed from all computers and devices.

Programmes should not be able to run automatically on computers and devices and should require administrator permissions.

Anti-malware programmes must run on all computers or devices that connect to the internet.

User accounts that are not needed must be removed from all computers and devices.

Anti-virus software must be updated as updates become available

All versions of software must be the latest version and supported by the manufacturer

When new software versions are made available by the manufacturer, they must be installed soon after they become available

Responsibility should be assigned for the management of the network as a critical asset for the organisation

Secure remote access must be in place to allow access to the network for remote workers

Appropriate encryption techniques should be employed for data at rest and in transit

# Procedural Controls

Information Security protocols and procedures will be issued to all **Practice** staff

Staff must undertake regular data security training and comprehension should be assessed and reported into the appropriate governance group within **The Practice**.

Access to physical buildings should be appropriately restricted and monitored to prevent unauthorised access

Where provided, staff must wear identity badges at all times

Staff must be careful when clicking on links or responding to unusual emails

Staff must not use **Practice** equipment for accessing sites unrelated to their work activities unless provided expressly permitted

# 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;

* 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 Incident Protocol
* Information Risk and Audit Protocol
* Data Protection Impact Assessment Protocol
* Freedom of Information Protocol

# Audit Schedule

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

# Review

This protocol will be reviewed every year or sooner where necessary

# Appendix A User Authorisation Process

**New Starter Authorisation Process**

1. New Starter form completed by line manager and sent to **The Practice** IT Provider
2. Logins are created for **The Practice**’s shared drive and any other key systems
3. New employee calls IT Provider on first day of employment and confirms identity via security questions
4. ‘one-time use’ password is provided verbally
5. Employee resets password as part of initial log in

**Password Reset Process**

1. Employee calls IT Provider service desk
2. Identity is verified via security questions
3. Password reset to ‘one-time use’ password which is provided verbally
4. Employee resets password as part of initial log in

**Staff Leaver De-authorisation Process**

1. Line manager logs a support request by email to IT Provider providing exit date of staff member
2. Logins are deactivated effective exit date
3. Folder access permissions are removed automatically
1. Information Security Management Principles 2nd Ed [↑](#footnote-ref-1)