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 |
| 1.2 | Emma Cooper, Kafico Ltd, DPO | Updated to include Email Security, Internet Security, Equipment Security and Use of Personal Devices. |

Contents

[2. Scope 2](#_Toc66882863)

[3. Definitions 2](#_Toc66882864)

[4. Introduction 3](#_Toc66882865)

[5. Statutory Mandatory Framework 3](#_Toc66882866)

[6. Accountable Parties 3](#_Toc66882867)

[7. Introduction 3](#_Toc66882868)

[8. Equipment Security and Integrity 4](#_Toc66882869)

[9. Email Security 4](#_Toc66882870)

[10. Internet Security 5](#_Toc66882871)

[11. Identity, Authentication and Authorisation 5](#_Toc66882872)

[12. Use of Personal Devices 6](#_Toc66882873)

[13. Setting up Personal Device Use for New Starters (laptops and computers) 7](#_Toc66882874)

[14. Accountability, Audit and Compliance 8](#_Toc66882875)

[15. Information Risk 8](#_Toc66882876)

[16. Technical Controls 9](#_Toc66882877)

[17. Procedural Controls 10](#_Toc66882878)

[18. Information Incidents 10](#_Toc66882879)

[19. Associated Protocols 10](#_Toc66882880)

[20. Review 10](#_Toc66882881)

[Appendix A User Authorisation Process 12](#_Toc66882882)

# 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 | Stanton (west) | Mendlesham |
| Burlington Road | Peninsula | Wickhambrook |
| Framlingham | Felixstowe Road Medical Practice | Church Farm Surgery (Aldeburgh) |
| Botesdale Health Centre | Ivry Street | Framfield |
| Hawthorn Drive | Lakenheath | Saxmundham |
| The Surgery, Leiston | Ixworth | Grove Medical Centre |
| Victoria Surgery | Little St John Street |  |

# 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**.

# Equipment Security and Integrity

* Staff are responsible for the security of the equipment that has been allocated to them or that they have access to, including any computer terminal and mobile devices, and they must be used in accordance with this protocol.
* Staff must lock screen or log off when leaving terminals or devices unattended.
* Anyone who is not authorised to access our network must only be permitted to use terminals or devices under supervision from Practice staff.
* The use of public WiFi for work purposes is not permitted as it is considered to be unsafe.
* If you have been issued with a laptop, tablet computer, smartphone, or other mobile device, staff must ensure that it is always kept secure, especially when travelling.
* Staff should not delete, destroy or modify existing systems, programs, information or data (except as authorised in the proper performance of your duties).
* Staff must not download or install software from external sources without authorisation from the Data Protection Lead. This includes software programs, instant messaging programs, screensavers, photos, video clips and music files.
* Staff must not attach any device or equipment to The Practice systems without authorisation from the Data Protection Lead. This includes any USB flash drive, MP3 player, tablet, smartphone or other similar device, whether connected via the USB port, infra-red connection or in any other way.
* Staff should inform the Data Protection Lead if staff suspect a virus. The Data Protection Lead may be required to delete or block access to emails or attachments in the interests of security.
* Staff should not attempt to gain access to restricted areas of the network, or to any password- protected information inappropriately.

# Email Security

* The Practice software monitors email traffic for viruses; however, staff should exercise particular caution when opening unsolicited or suspicious emails from unknown sources.
* Email messages may be required to be disclosed in legal proceedings in the same way as paper documents and can be retrieved even once deleted.
* Staff who receive an email in error should inform the sender and delete the erroneous email.
* Staff should not use their own personal email account to send or receive email for the purposes of The Practice business.
* When sending email that contains sensitive or service user data, staff should always use a secure email service – such as NHS Mail.
* When sending email from NHS Mail account to a non-secure recipient email account such as Hotmail, staff should insert [secure] into the subject line to enable encryption.
* Where available, The Practice staff should use the confidentiality labels and encryption function for individual emails where appropriate, using the Encrypt button at the top of a new email.

Senders can then select from;

* + Encrypt Only
	+ Do not forward.
	+ Confidential / All Employees
	+ Highly Confidential

# Internet Security

* Internet access via The Practice devices is provided primarily for business purposes. Incidental and occasional personal use of the internet, email, and telephone systems is permitted, but should only involve access to trusted sites and appropriate content.

# Identity, Authentication and Authorisation

* Default passwords (factory settings) on all equipment have been amended by the CSU 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 will be implemented to ensure that access is limited to the correct individuals and the correct information assets.

# Use of Personal Devices

* Line Managers are responsible for ensuring that:
	+ Staff have an appropriate business need to use their personal device for work and that other options are not available (such as IT issued devices).
	+ Staff comply with this protocol and associated procedures.
	+ the correct process is followed to on-board staff which typically starts with a service request to the IT Service Desk
	+ They take disciplinary action as appropriate against any member of staff in breach of this protocol.
	+ notify any suspected breaches of this protocol to the Data Protection Officer
	+ Immediately notify the appropriate IT Lead if a staff member leaves or no longer requires use of their personal device for work purposes.
	+ Follow the Leaver’s Process to remove access to software and systems as appropriate.
* Practice who are using their own device for work purposes, must, without exception;
	+ Abide by this and associated policies & procedures.
	+ Report any suspected breaches of this protocol to their line manager or the Data Protection Officer
	+ Understand that failure to comply with the rules contained in this protocol, or any attempt to circumvent the security controls, may result in the withdrawal of this facility and/or disciplinary action.
	+ Report the loss or theft of a personal device being used for work purposes to their line manager at the earliest possible opportunity.
	+ Inform the IT Service Provider if use of personal device for work purposes is no longer required and access to the applications will be removed and relevant data deleted.
	+ Report any lost or stolen devices to line manager and Data Protection Officer immediately
	+ Keep their username and password secret and not allow anybody else to access the information.
	+ Take suitable precautions to protect the physical asset in transit and in work locations.
	+ Not use a shared / communal device
	+ Not storing personal/confidential patient information on the device unless absolutely necessary and appropriate security is in place.
	+ Safely transfer information to the appropriate health and care record as soon as it is practical to do so.
	+ Avoid downloading software or videos / open suspicious links
	+ Where provided, use software such as Away from my desk / VPN
	+ Not print out documents on home printer, instead store in shared drive
	+ Log out of all software and systems, including emails, when not in use
	+ Within NHS Mail, only view documents in browser and do not download
	+ Where possible create a normal “user” account on the laptop without admin capabilities to undertake the work
	+ Additionally, no documents should be downloaded to the laptop unless absolutely necessary, attachments to emails can be viewed in browser but there may other systems or portals accessed that permit the download of documents.
	+ If documents can be viewed online staff should only do so
	+ If it is necessary to download, staff should delete their download history and empty their recycling bin at the end of each work session.

# Setting up Personal Device Use for New Starters (laptops and computers)

* Whereas IT issued devices are configured for appropriate security and remote management, this is not in place for personally owned devices and so particular steps are taken to reduce the risk to practice data.
* When a new member of staff joins the practice, the Management Team will make enquiries around whether a practice issued device will be issued to the new starter.
* Where it is confirmed that the staff member will be using their own device, management must perform the following checks regarding the personal device;
	+ Confirm that anti-virus software is installed and will automatically update.
	+ Confirm that encryption software is in place.
	+ Confirm that device access controls are in place.
	+ Ensuring that access to practice data is via web browser and that no materials are downloaded to the device itself.
* For use of personal mobile phones, the following will be checked;
	+ Staff will not take patient photographs directly on their phone, outside of specialist, practice approved software that facilitates photography.
	+ Change Default Passwords / Pins on the mobile
	+ Use Two-Factor authentication where available.
	+ Remove any Unused Apps from Personal Mobiles and only Download Trusted Apps
	+ Ensure that staff access to software is removed when the individual leaves the practice.
* Following the review, risks or issues will be reported by the line manager to the SIRO and DPO.
* Following the review, evidence of the review must be retained by the practice.

# Accountability, Audit and Compliance

Information Assets Owners must be allocated for all key information assets and are responsible for monitoring risk, alerting the Data Protection Lead 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 organisation’s information assets.

The impact of the threats must be considered at the appropriate **The 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 **The 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;

* 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

# 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 **[insert]**
2. Logins are created for **The Practice**’s shared drive and any other key systems
3. ‘one-time use’ password is provided verbally
4. Employee resets password as part of initial log in

**Password Reset Process**

1. Employee calls **[insert]**
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 **[insert]** 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)