### INFORMATION SECURITY POLICY

### FOR USE IN

### ST JOHN’S WAY MEDICAL CENTRE

### 96 St John’s Way, London N19 3RN

**PRACTICE CALDICOTT LEAD:**

**Dr Chris Cooper, GP Principal**

Version 2.2

Author: PCT Policy, customised by PJB

**1. INTRODUCTION**

1.0 This document is a statement of policy of St John’s Way Medical Centre. The purpose of this policy is to recognise the security threats to information and to provide a framework for reducing the likelihood of security incidents. It provides high level guidance on ensuring the confidentiality, integrity and availability of information.

1.1 Policy Statement. The Practice will seek to ensure the confidentiality, integrity and availability of its information is maintained by implementing best practice to minimise risk.

1.2 Requirement for Security Policy. Information, and the IT systems that support it, represent an increasingly valuable asset as systems proliferate and increased reliance is placed on them. The Practice seeks to protect its information systems from misuse and to minimise the impact of service breaks by developing a Security Policy and procedures to manage and enforce it. Key issues addressed by the Security Policy are:-

**Confidentiality** - data access is confined to those with specified authority to view the data;

**Integrity** - all system assets are operating correctly according to specification and in the way the current user believes them to be operating;

**Availability** - information is delivered to the right person when it is needed.

1.3 Scope of Policy. The Practice policy aims to ensure that its information systems are properly assessed for security, that the confidentiality, integrity and availability of information is maintained and their staff are fully aware of their responsibilities, roles and accountability and procedures to detect and resolve security breaches are in place. The policy relates to information held in both manual and electronic form.

1.4 Legal Compliance. The Practice is bound by the provisions of a number of items of legislation affecting the stewardship and control of patient and other information. The main relevant legislation is:

* The Data Protection Act 1998;
* Access to Health Records Act, 1990 (where not superseded by the Data Protection Act, 1998);
* The Freedom of Information Act 2000;
* Computer Misuse Act, 1990;
* GDPR, May 2018

This policy describes the way in which information should be managed, in particular, the way in which personal or sensitive information should be protected.

The Practice and all its staff are bound by their duty of confidentiality, this includes the Caldicott guidance on protection of patient information.

1.5 Information Governance. Information Governance can be described as a framework for handling information in a confidential and secure manner to the appropriate ethical and quality standards. It brings together Caldicott, Data Protection, Freedom of Information and Information Security, as well as other related disciplines.

**2. SECURITY MANAGEMENT**

Objective: to establish the management structure for information systems security within The Practice.

*Rationale – in order for information in The Practice to be properly controlled and protected, it is extremely important that individuals and organisations are clear about who owns specific items of information and/or information systems. Within The Practice, the security of information will be managed professionally and to the highest standards. Owners will be identified for specific information systems and, where appropriate, specific datasets. These owners will work with Caldicott Guardians to determine appropriate data sharing protocols, access protocols and appropriate security practices and procedures.*

2.1 Information Security Management System. Overall responsibility for Information Security rests with the designated lead. That person will have security management responsibilities for the following areas:

* monitoring and reporting on the state of information security within the Practice;
* ensuring that the Information Security Policy is implemented throughout the Practice;
* developing and enforcing detailed procedures to maintain security;
* ensuring compliance with relevant legislation;
* ensuring that staff are aware of their responsibilities and accountability for information security;
* carrying out initial investigation and reporting into any breach or suspected breach of security.

2.2 Caldicott. The designated Caldicott Guardian has a particular responsibility for ensuring that everyone in their organisation conforms to the Caldicott Principles regarding the protection and use of patient identifiable information.

**3. ENABLING THE FLOW OF INFORMATION**

#### Objective: to enable the efficient flow of information without compromising its integrity and confidentiality

Rationale - information routinely flows within the NHS community and between NHS organisations and other bodies concerned with patient care or an individual’s medical condition. The routine use of patient identifiable information for non-clinical purposes could have an adverse effect on the doctor/patient relationship. It could also infringe individuals’ rights to have confidential information about them used properly. With this in mind the practice has established a Caldicott Guardian to ensure that the flow of patient identifiable information is appropriately controlled.

3.1 Patient identifiable information. The Practice is to be fully committed to the Caldicott Principles regarding the protection and use of patient-identifiable information, namely:

* Use and transfer of such information will only take place where the purpose is fully justified;
* Use and transfer will only occur when absolutely necessary;
* Use the minimum required – where possible, all data should be anonymised;
* Access strictly “need to know”;
* Everyone must understand their responsibilities;
* Understand and comply with the law.

**4. COMMUNICATIONS**

Objective: to ensure that The Practice uses electronic, postal and verbal communications appropriately.

*Rationale – the use of IT networks will continue to increase and will become the primary means of communication within and between the various organisations providing services to patients throughout the Health Community. One consequence of this is that the networking infrastructure will be increasingly used for a wide variety of purposes to facilitate more flexible working practices and delivery of care. Specific examples in this area include homeworking by both clinical and managerial staff. Domestic dwellings may be more vulnerable than work premises to theft and subsequent loss or disclosure of information. Increased use of fax and email also introduces the vulnerability to interception or misdirection. It is appropriate to include postal and verbal communications as part of an information security policy as these elements are integral parts of the information management culture.*

4.1 Connectivity. The Practice will comply with the NHS Code of Connection**.** The NHS WAN connection (N3 currently) is the responsibility of the PCT and the PCT ensures compliance. Should practices wish to make any additional network connections, they must ensure that these conform with the Code of Connection requirements.

4.2 Homeworking. The Practice has a set of strict controls and procedures which apply to all homeworking activity. Only those members of staff prepared to implement the controls and certify that they have done so will be permitted to use official equipment at home. SEE POLICY

4.3 Telephone Security. It is essential that all staff are aware of the need to check on the credentials and identity of all callers requesting patient-identifiable or other sensitive information. See separate Telephone Policy.

4.4 Internet and E-mail use. The Practice recognises the use of the Internet and e-mail as a legitimate business tool and one that can have huge benefits if used correctly. At the same time there are significant dangers involved that must be borne in mind by all users when using Internet and e-mail facilities. All users must comply with the Acceptable Internet Policy and Acceptable E-Mail Policy. SEE POLICY

**5. SECURITY RESPONSIBILITIES**

##### Objective: to ensure that staff are aware of security risks and their responsibilities to minimise the threats.

*Rationale – information security is a shared responsibility. Confidentiality, integrity and availability of information could be compromised due to a breach of security (which could be accidental or malicious) occurring at any point in the information flow cycle.*

5.1 Management Responsibilities. It is the responsibility of the designated Practice IT lead to ensure the following in relation to their staff:

* All current staff should be instructed in their security responsibilities.
* Staff using computer systems must be trained in their use.
* Staff must not be able to gain unauthorised access to any of The Practice’s IT systems.
* Practice IT lead should determine which individuals are to be given authority to access specific computer systems. The level of access to specific systems should be on a job function need.
* Current documentation must be maintained for all critical job functions to ensure continuity in the event of relevant staff being unavailable.
* Staff should have security responsibility included in their contract of employment.
* The Practice Manager must ensure that all contractors undertaking work for or on behalf of organisations within The Practice have signed confidentiality (non-disclosure) undertakings.

5.2 Staff Responsibilities. Each member of staff is personally responsible for ensuring that no breaches of information security result from their actions. Failure to do so may result in disciplinary action and may be considered gross misconduct.

5.3 Training. The Practice IT lead will have specific responsibility for the overall security awareness of the Practice and is specifically to ensure that all staff have security awareness training.

**6. EQUIPMENT SECURITY**

**Objective: to protect IM&T equipment against loss or damage and avoid interruption to business activity**

6.1 Equipment siting and protection. IM&T equipment should always be installed and sited in accordance with the manufacturer’s specification.

6.2 Physical security. All physical security of equipment lies with the practice.

Local network equipment, file servers and NHSNet terminating equipment should be located in secure areas and/or lockable cabinets.

**7. USERS’ ACCESS CONTROL**

Objective: to control individuals’ access to systems and manual libraries according to the requirements of their job function

*Rationale - the need for carefully controlled access to the information held on computerised information systems or in manual files, reports and other written communications is a central tenet of information security. The Caldicott report on the protection and use of patient-identifiable information recognises this, and a core responsibility of the Caldicott Guardians is to define and assign access privileges to systems and their users. Guardians will be assisted in this task by individual system owners.*

7.1 Registering users for access to systems. All users of The Practice IT systems will be required to complete a formal authorisation process. Once completed and approved an account will be set up by the will identify those systems, manual files, applications and networks which contain information to which access should be restricted, and will apply appropriate authentication controls commensurate with the sensitivity of the data held within or transmitted across them. Formal procedures will be used to control access to systems.

7.2 Password management. Passwords are a cornerstone of the security of The Practice IT systems. Strong passwords are a vital part of ensuring that information held on our systems is secure in accordance with legislation. Weak or incorrectly stored and shared passwords provide a significant weak link in our security framework.

7.3 User Accounts & Log Ins. It is a basic premise of computer systems that an individual user logs on with a unique ID, and using a password known only to them. Any actions carried out by that user are then logged by the system and legally attributable to them until such time as they log off.

**8. SECURITY INCIDENT MANAGEMENT**

**Objective: to detect, investigate and resolve any suspected or actual information security breach**

*Rationale – part of the effective management of security risks involves the logging and resolution of incidents. This allows incidents to be investigated fully with conclusions and recommendations drawn from them and, where required, remedial action to be taken.*

8.1 Security incidents. A security incident is an event that may result in:

* degraded system integrity;
* loss of system availability;
* disclosure of confidential information;
* disruption of activity;
* financial loss;
* legal action;
* unauthorised access to applications.

8.2 Individuals’ responsibilities. All those working within the practice are personally responsible for ensuring that no actual or potential security breaches occur as a result of their actions. They should ensure that they do not disclose their passwords or allow anyone else to use their password or allow another user to work under their log on. In addition this should ensure that all confidential material is kept secure.

8.3 Incident reporting. All incidents involving IT systems should be reported locally in the first instance to the Practice IT lead. Incidents should then be reported to the IT Helpdesk if they require technical assistance. All incidents should be treated as significant events.

**9. OPERATIONAL CONTROLS & HOUSEKEEPING**

#### Objective: to maintain the integrity and availability of information assets

*Rationale – housekeeping is an integral part of the security equation. Lost or destroyed information could have a detrimental effect on the service provided or on the treatment of individuals. Effective operational controls and housekeeping mean that the availability of The Practice’s information base will be preserved. The housekeeping principle applies to both manual information, e.g. records management, manual filing systems, and to electronically held information.*

9.1 Data backup. All systems are to have appropriate backup regimes which reflect the importance of the data and which have been subjected to a proper risk assessment. SEE POLICY.

9.2 Virus & Spyware control. The Practice seeks to minimise the risks of computer virus through user education, good practice and up to date effective anti-virus software. Users need to be aware that no newly acquired disks from whatever source, are to be loaded unless they have previously been virus checked according to their organisation’s policy on protection of data. Anti spyware is currently the responsibility of the practice.

9.3 Controlled stationery. e.g. payment stationery, drug ordering, prescriptions etc. Formal procedures should be established to control and account for the use of such stationery.

9.4 Media disposal. Any storage media which is being disposed of either by destruction or for re-use must have all data permanently removed from it. This is a specialist IT task which must be carried out under strict control.

**10. QUALITY CONTROL AND DATA VALIDATION**

**Objective: to maintain confidence in data accuracy for use in decision making**

*Rationale – the integrity of data is a key component of information security. Therefore it is vitally important that data held by The Practice is of the highest possible quality. Inaccuracies in data, particularly that relating directly to patient care, may adversely affect a patient’s treatment or seriously disrupt the running of the practice’s operations. This requirement extends to both computerised and manual data.*

10.1 At data input. Data accuracy is the direct responsibility of the person entering the data, supported by their line manager. Error correction should be done at the source of input or as soon as it is detected. Any loss or corruption of data should be reported to the GP IT Helpdesk or supplier at once - this should involve incident recording mechanisms immediately and possibly major incident control (dependant upon the severity of the problem). Systems developed/purchased by the practice need to take that this into account and provide adequate validation.

10.2 Internal validation. All systems will incorporate internal validation processes and audit trails to detect and record problems with processing or data integrity.

**11. SOFTWARE SECURITY**

**Objective: to comply with the law on licensed products and minimise risk of computer virus infection**

*Rationale – legislation on protection of software is strict. Prosecutions can be costly for organisations and abuse by employees constitutes a disciplinary offence. In addition, illegally obtained software can be a source of virus infection (see also section on operational controls and housekeeping).*

11.1 Licensed software. Only licensed software to be used on practice PCs. Any software should only be loaded with the permission of the IT lead. Any breach may be subject to disciplinary procedure and possibly gross misconduct.

11.2 Organisation software standards. The Practice will only permit approved software to be installed on their PCs.

**12. IT DISASTER RECOVERY & BUSINESS CONTINUITY PLANNING**

Objective: to maintain business continuity and restore computer facilities for essential activities following a major failure or disaster

*Rationale – The Practice’s information systems are at risk from a variety of sources which threaten the confidentiality, integrity and availability of information and data. In order to limit the consequences of any threat and to maintain continuity of operations, a business continuity plan will be developed and maintained.*

12.1 Need for effective plans. The Practice recognises that some form of disaster may occur, despite precautions, and therefore seeks to contain the impact of such an event on its core business through tested disaster recovery plans. It is recognises that IM&T systems are increasingly critical to its business and that the protracted loss of key systems or user areas could be highly damaging in operational terms. It is essential therefore that tried and tested disaster recovery plans for its computing facilities to be maintained.

12.2 Planning process. The main elements of this process will include:

* identification of critical computer systems;
* identification and prioritisation of key users and user areas;
* agreement with users to identify disaster scenarios and what levels of disaster recovery are required;
* identification of areas of greatest vulnerability based on risk assessment;
* mitigation of risks by developing resilience;
* developing, documenting and testing disaster recovery plans identifying tasks, agreeing responsibilities and defining priorities.

12.3 Planning framework. Disaster recovery plans will cater for different levels of incident including:

* emergency procedures covering immediate actions to be taken in response to an incident (e.g. alerting disaster recovery personnel);
* fallback procedures describing the actions to be taken to provide contingency devices defined in the disaster recovery plan;
* resumption procedures describing the actions to be taken to return to full normal service;
* testing procedures describing how the disaster recovery plan will be tested.

**13) NATIONAL DATA OPT-OUT FOR HEALTH AND CARE DATA**

## A system of opt-out for use of health and care personal data (including pseudonymised data) has been implemented by the NHS. We are required to comply with this. We will therefore:

## Ensure that all data extracts for non-direct care purposes are filtered to remove patients who have opted out

1. Ensure that we make patients aware of their rights.
2. Where data is being manually extracted for non-care purposes, we will ensure that records are manually checked for opt-out

**14) DATA PROTECTION BY DESIGN AND DEFAULT**

## The GDPR requires that all use of personal data includes “Data protection by design and default” (Article 25). To ensure this is carried out we will:

1. Implement appropriate technical and organisational measures to implement the data protection principles
2. Ensure that such measures are kept under review and regularly checked to ensure they still meet the requirements, learning from processing and changes in the state of the art
3. Ensure in particular that we minimise the personal data held and restrict access strictly to that required for the purpose of processing
4. To these end, we may employ certifications as an element to demonstrate compliance where approved by the regulators (Article 42)

##### APPENDICES

* Internet &Email Policy
* Back Up Policy
* Homeworking Policy
* Management & Retention of Records
* Telephone Security Policy
* Confidentiality Agreement