INFORMATION GOVERNANCE AND DATA SECURITY POLICY 2018-19

Document History

Version Date:	October 2018
Version Number:	1.0
Status:	DRAFT
Next Revision Due:	December 2019
Developed by:	Paul Couldrey (IG Consultant)
Policy Sponsor:	
Approved by:	
Date approved:	
Date ratified:	

Revision History

Version	Revision date	Summary of Changes
0.1	08/02/18	First Draft

Introduction
Red House recognises that information has its greatest value when it is accurate, up to date and accessible where and when it is needed. Inaccurate, outdated or inaccessible information that is the result of one or more information security weaknesses can quickly disrupt or devalue critical processes. Information underpins the delivery of high quality healthcare commissioning and many other key service deliverables. In addition, the public is increasingly concerned about how organisations are handling information; the patients have a right to expect us to handle their data in a safe and secure manner and comply with legal and professional responsibilities.

There is a legal requirement for the practice as a Public Authority to address compliance with the incoming General Data Protection Regulation (GDPR) by 25 May 2018, and the Associated UK specific Data Protection Act 2018 together with associated (to be published NHS guidance).

An effective information security management regime must be in place to ensure that information is appropriately protected and reliably available.

This document sets out a strategic direction for information governance management within THE PRACTICE.

The policy is based on a number of legal and best practice standards including:

- ISO27001, the international standard for information security management systems (ISMS)
- Information Security Management: NHS Code of Practice
- General Data Protection Regulation 2016, Data Protection Act 2018, Freedom of Information Act 2000, Computer Misuse Act and other related law and regulation
- Health and Social Care Act 2013
- NHS Act 2006 (s.251 and associated CAG Approvals)
- Office of Government Commerce (OGC) Policies & standards
    - Information Technology Infrastructure Library (ITIL)
    - Communications- Electronics Security Group (CESG) Guidance
    - Management of Risk

THE PRACTICE is committed to ensuring that there is adequate provision for the secure management of information resources it owns or controls.

THE PRACTICE recognises that information security is not simply about implementing Information technology solutions; it reflects overall management and the culture of the organisation.

Scope

This policy relates to:

- all information that is processed or held during the practice business or on its behalf by key providers;
- the handling of all information through all recognised means; and
- all information systems purchased, developed and managed by or on behalf of the THE PRACTICE.

It also applies to all members of staff employed by, or working on behalf of the THE PRACTICE, including contracted, non-contracted, temporary, honorary, secondments, bank, agency, students, volunteers, locums or third parties.

The Information Governance Policy recognises that the practice is an organisation working within a new and rapidly changing commissioning and information governance landscape, especially with the introduction of the GDPR. As such the PRACTICE's policy is focused on setting up and embedding the required governance arrangements and doing this in such a way that the practice retains the maximum flexibility and resilience so that it can adapt to this environment.

The key elements and resources to support the delivery of this policy are:

- The Information Governance Toolkit, and subsequent Data Security and Protections Toolkit (2018);
- Information Governance Management Framework and Policy
- GDPR PID and Improvement Plans (High Level and Operational)
- Information Governance Policy;
- Information Governance Policies;

The Information Governance Improvement Plan, identifying lead the practice officers, will be agreed each year to ensure compliance against each of the requirements. This Plan forms part of the overall practice endorsed Data Protection and Confidentiality Policy.

Purpose

The purpose of this policy is to describe the management arrangements that will deliver Information Governance assurance for THE PRACTICE. Information Governance is a framework that enables the organisation to establish good practice around the processing of information and use of information systems, ensure that information is handled to ethical and quality standards in a secure and confidential manner, promote a culture of awareness and improvement, deliver its corporate objectives and comply with legislation, statutory requirements and other mandatory standards.

The Information Governance Management Framework (IGMF) will underpin the PRACTICE's strategic goals and ensure that the information needed to support and deliver their implementation is readily available, accurate and understandable.

Information Governance has four fundamental aims:

- To support the provision of high-quality care by promoting the effective and appropriate use of information;
- To encourage responsible staff to work closely together, preventing duplication of effort and enabling efficient use of resources;
- To develop support arrangements and provide staff with appropriate tools and support to enable them to carry out their responsibilities to consistently high standards;
- To enable the practice to understand its own performance and manage improvement in a systematic and effective manner.

THE PRACTICE has a statutory responsibility to patients and the public to ensure that the services it provides have effective policies, processes and people in place to deliver objectives in relation to holding and using confidential and personal information. be embedded in the contracting process.

Broad Objectives

THE PRACTICE will ensure there is a systematic and planned approach to the management of information governance by establishing an Information Security Management System (ISMS) in line with ISO27001 and Information Security Management: NHS Code of Practice.

- The effectiveness of the ISMS will be continually improved through the use of audit results, analysis of incidents, corrective and preventive actions and management reviews.

- All important information assets will be identified and appropriately managed and protected. Any protection applied will be based on formally documented risk assessments to ensure that it is commensurate with the value of the asset and the perceived threats.

- Actual and potential information governance related incidents will be recorded and responded to in a timely and appropriate manner; findings will be fed into the ISMS to ensure continued and ongoing improvements.

- Steps will be taken to ensure that internal and external transfers of patient confidential information are conducted in a secure and safe manner, this will include, for example, encryption of emails and removable media holding personal information (as mandated by the Cabinet Office Information Governance Assurance Programme in 2008).

- All staff, contractors and other relevant parties will be made aware of the organisations requirements for information security and undertake appropriate training.

- A culture of information security awareness will be promoted and established.

- Procedures will be established to ensure that information governance requirements are addressed during the implementation, development and maintenance of services and/or systems.

- Business continuity plans will be developed across all services to ensure the centre is able to continue with its core business functions in the event of a failure or loss of systems or services. Appropriate procedures will be developed to ensure the timely recovery or replacement of information systems and services. The plans will be regularly tested and revised.

- Systems and services will be regularly audited against information governance related policies and procedures. The results of such audits will be fed into the ISMS, the Information Governance work-plan and information risk registers to ensure continued and ongoing improvement.

Information Security Management System (ISMS)

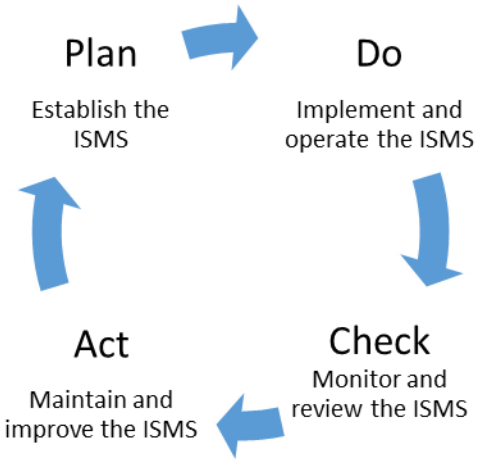
THE PRACTICE recognise that effective information security involves more than simply installing security products such as anti-virus software and providing a security policy. The practice will establish an ISMS, which will provide a means to identify and co-ordinate the approach to the management of information security within the practice in order to protect it, and its business.

The ISMS will be based on the NHS Information Security Management Framework.

The governing principle behind the ISMS is the design, implementation and maintenance of a coherent set of policies, processes and systems to manage risks to its information assets, thus ensuring acceptable levels of information security risk.

Based on this risk approach, we will establish, implement, operate, monitor, review, maintain and improve information security for all organisations within the PRACTICE.

The Core Elements of an effective Information Security Management System are summarised in the following Plan-Do-Check-Act model.



PLAN - Establish the ISMS

- Define the business needs for information security and set those out in a corporate Information Security Policy
- Identify and assess the risks to Information Security
- Identify and evaluate controls to be established to manage the information security risks identified, transfer the risks or accept them as appropriate.

DO - Implement and operate the ISMS

- Develop and implement action plans to manage the identified information security risks
- Implement training and awareness for all relevant staff

CHECK - Monitor and review the ISMS

- Establish processes to identify actual and potential information security incidents or system weaknesses
- Monitor and update information security risk assessments as required
- Monitor the effectiveness of the ISMS in managing information risks through internal reviews and independent audit.
- Report the results to management for review.

ACT - Maintain and improve the ISMS

- Take corrective and preventative actions, based on the results of audits and management reviews or other relevant information, to achieve continual improvement of the ISMS.

Following the principles of the above model, an Information Governance Work-plan for the practice will be created. This encompasses the requirements of the Information Governance toolkit (DS&P Toolkit), legal and NHS requirements and the results of audits and risk assessments. The work-plan will be carefully monitored and regularly reviewed and revised, to ensure it continues to meet the information governance requirements of the practice and ensure continuous improvement.

Governance Arrangements

An information governance steering group has been established (Terms of Reference in Appendix 1) to ensure that information security goals are identified, meet the organisational requirements, and are integrated in relevant processes and work plans.

The group will be accountable to the practice Information Governance Steering Group will perform the following functions:

- Develop and maintain the information governance policy and supporting policies, procedures and guidelines.
- Conduct regular audits to review the effectiveness of the implementation of the information governance policy.
- Provide clear direction and visible management support for security initiatives.
- Identify the resources needed for information governance.
- Approve assignment of specific roles and responsibilities for information governance across THE PRACTICE.
- Initiate plans and programmes to maintain information security awareness.
- Ensure that the implementation of information security controls is coordinated across THE PRACTICE.
- Take appropriate action and implement any necessary changes to policy or procedures in response to the results of audits or incidents.
- Continually monitor and assess risks, ensuring appropriate and timely responses to changing and emerging threats.

Information Governance Definition

Information Governance is “a framework for handling information in a confidential and secure manner to appropriate ethical and quality standards in modern health services”. It brings together within a singular cohesive framework, the interdependent requirements and standards of practice. This policy forms part of THE PRACTICE’s overall Practice Assurance Framework.

IG is defined by the requirements that the organisation is required to demonstrate compliance with as part of the IG Toolkit Annual Assessment (DS&P toolkit from 2018), these include the following domains:

- Information Governance Management
- Confidentiality and Data Protection Assurance
- Information Security Assurance
- Clinical Information Assurance
- Secondary Use Assurance

Within this definition and domains the practice will handle and protect many classes of information:

- Some information is confidential because it contains personal details the practice must comply with regulation which regulates the holding and sharing of confidential personal information. Changes to the way in which patient confidential data can be processed came about as a result of the Health & Social Care Act 2012. It is important that relevant, timely and accurate information is available to those who are involved in the care of service users, but it is also important that personal information is not shared more widely than is necessary;
- Some information is non-confidential and is for the benefit of the practice and the general public and its employees share responsibility for ensuring that this type of information is accurate, up to date and easily accessible to the public;
- The majority of information about the practice and its business should be open to public scrutiny although some, which is commercially sensitive, may need to be safeguarded.

Information can be in many forms, including (but not limited to):

- Structured record systems – paper and electronic;
- Transmission of information – fax, e-mail, post and telephone; and
- All information systems purchased, developed and managed by/or on behalf of the THE PRACTICE.

Aims & Objectives

The IG Policy of the practice will be based upon a vision of a long-term delivery of clear, open aims and objectives to ensure that:

- The practice complies with all statutory requirements;
- The practice has an information governance policy that supports the achievement of corporate objectives;
- The practice can demonstrate an effective framework for managing information governance assurance;
- Staff are aware of their responsibilities and the importance of information governance;
- Information governance becomes a systematic, efficient and effective part of business as usual for THE PRACTICE;
- Information governance is integrated into the change control process;
- There are effective methods for seeking assurance across the organisation;
- THE PRACTICE can demonstrate that the information governance arrangements of organisations it commissions services from across healthcare and commissioning support are adequate;
- The policy is able to respond to any change required by external bodies and any challenges emerging from changes to the information governance landscape.

An outline of the high-level IG organisational objectives that the practice seeks to achieve is as follows:

- Comply with the relevant information privacy and confidentiality laws and regulations as well as contractual requirements and internal policies on information and systems security and protection, and provide transparency on the level of compliance via the DS &P Toolkit;

- Maintain information risk at acceptable levels and protect information against unauthorised disclosure, unauthorised or inadvertent modifications, and possible intrusions;

- Address the increasing potential for civil or legal liability impacting the organisation as a result of information breaches through efficient and effective risk management, process improvement and rapid incident management;

- Provide confidence in interactions with key external organisations – for example, Acute & Community Providers, customers, NHS England, NHS Digital, Monitors, Commissioners and the CQC.

- Create, maintain and continuously improve trust from customers and the public;

- Provide accountability for safeguarding patient and other critical information; and

- Protect the organisation’s reputation.

These aims, and objectives will be achieved by ensuring the effective management of Information Governance by:

- Ensuring that the practice meets its obligations under the Data Protection legislation, the Human Rights Act 1998, the Freedom of Information Act 2000 and the Health and Social Care Act 2012;
- Establishing, implementing and maintaining policies for the effective management of information;
- Ensuring that information governance is a cohesive element of the internal control systems within THE PRACTICE;
- Recognising the need for an appropriate balance between openness and confidentiality in the management of information;
- Ensuring that information governance is an integral part of the practice culture and its operating systems;
- Ensuring maintenance of year on year improvement within the Information Governance Toolkit submission;
- Reducing duplication and looking at new ways of working effectively and efficiently;
- Minimising the risk of breaches of personal data;
- Minimising inappropriate uses of personal data;
- Ensuring that Service Level Agreements between the practice and other organisations are managed and developed in accordance with Information Governance Principles;
- Ensuring that contracted bodies are monitored against Information Governance standards;
- Protecting the services, staff, reputation and finances of the practice through the process of early identification of information risks and where these risks are identified ensuring sufficient risk assessment, risk control and elimination are undertaken;
- Ensuring there is provision of sufficient training, instruction, supervision and information to enable all employees to operate within information governance requirements, including those undertaking specialist roles;
- Ensuring the information governance policy and related plans link to and support other corporate or strategic objectives, e.g. business continuity planning, and ensuring the practice is able to meet its commitments under the Civil Contingencies Act 2004 (specifically the Emergency Preparedness, Resilience & Response assurance process).

Roles and Responsibilities

Information Governance Steering Group

The Information Governance Steering Group will be established to support and drive the broader information governance agenda and provide the partners with the assurance that effective information governance best practice mechanisms are in place within THE PRACTICE.

The IGSG will meet every 6 months and will be Chaired by the SIRO. The Group will:

- be accountable to the Senior partners
- support the practice SIRO and the practice Caldicott Guardian in their roles;
- monitor information governance performance annually using the DS & P Toolkit hosted by NHS Digital (NHSD);
- provide audited toolkit Results to the partners for approval prior to final submission to the NHSD;
- be responsible for overseeing operational information governance issues;
- develop and maintain policies, standards, procedures and guidance;
- co-ordinate and monitor the implementation of the information governance policy, framework and policies across the PRACTICE;

In addition to the SIRO, the membership of the IGSG will include the following:

- Senior Information Risk Owner (SIRO)
- Caldicott Guardian
- General Manager

(Terms of Reference in Appendix 1)

Individual roles

Senior Information Risk Owner (SIRO)

The SIRO for THE PRACTICE, holds responsibility for ensuring that information is processed and held securely throughout the PRACTICE. The role covers all the aspects of information risk, the confidentiality of patient and service user information and information sharing. The Information Governance Toolkit sets out clear responsibilities of the SIRO in relation to risks surrounding information and information systems, which also extend to business continuity and the role of Information Asset Owners.

In particular, the SIRO is responsible for:

- leading and fostering a culture that values, protects and uses information for the success of the practice and benefit of its service users;
- owning the PRACTICE's overall information risk policy and risk assessment processes and ensuring they are implemented consistently by Information Asset Owners (IAO's);
- take ownership of information risk assessment processes, including the review of the annual information risk assessment and agree actions in respect of any risks identified;
- ensure that THE PRACTICE's approach to information risk is effective in terms of resources, commitment and execution and that this is communicated to all staff;
- Ensure Information Asset Owners (IAOs) undertake risk assessments of their assets;
- Be responsible for the Incident Management process ensuring identified information security risks are addressed and any lessons learnt are implemented;
- Provide a focal point for the management, resolution and/or discussion of information risk issues;
- Ensure that the PRACTICEs approach to information risk is effective in its deployment in terms of resource, commitment and execution and that this is communicated to all staff;
- Ensure the organisation is adequately briefed on information risk issues

Caldicott Guardian

The Caldicott Guardian is responsible for acting as a champion for data confidentiality. They should ensure that confidentiality issues are appropriately reflected in practice policies and working procedures for staff and oversee all arrangements, protocols and procedures where confidential information may be shared with external bodies including disclosures to other public sector agencies and other outside interests.

The Caldicott Guardian is responsible for:

- ensuring that the practice satisfies the highest practical standards for handling patient information;
- ensuring confidentiality is reflected appropriately in THE PRACTICE's policies and procedures to support the lawful and ethical processing of information;
- acting as the 'conscience' of THE PRACTICE;
- ensuring that staff comply with Caldicott Principles and the guidance contained in the NHS Confidentiality Code of Practice;
- facilitating, enabling and overseeing information sharing agreements and arrangements put in place to share personal confidential data with external bodies.

Information Asset Owners

The Information Asset Owners (IAO) will be senior members of the practice staff responsible for information assets within their remit. They will provide assurance to the SIRO that information risk is managed effectively for their information assists. This will be achieved by:

- Ensuring all Information Assets and flows of data within their remit are identified and logged ensuring each has a legal basis to be processed.
- Identifying, managing and escalating all information security (for example, dependencies and access control) and information risks as appropriate.
- Supporting Information Asset Administrators who will ensure the above takes place. The detailed roles and responsibilities are defined in Appendix A of the NHS Information Risk Management Guidance
- Ensuring that information risk assessments are performed on all information assets where they have been assigned 'ownership' and provide assurance to the SIRO on the security and use of these assets;
- Knowing what information is held and for what purpose;
- Ensuring that information governance policies and system level procedures are followed.

All staff (and Third Parties)

All those working for the practice have legal obligations, under the Data Protection legislation, common law duty of confidentiality, and professional obligations, for example the Confidentiality NHS Code of Practice and professional codes of conduct. These are in addition to their contractual obligations which include adherence to policy, and confidentiality clauses in their contract.

The same responsibilities apply to those working on behalf of the organisations whether they are volunteers, students, work placements, contractors or temporary employees. Those working on behalf of the organisation are required to sign a third-party agreement outlining their duties and obligations.

Breaches of any law, contract, code of practice or confidentiality agreement will be reported using appropriate channels and action taken where necessary.

Information Governance Toolkit

Completion of the Information Governance Toolkit (IGT) is mandatory for all organisations using NHS Mail and providing NHS services. The IG Toolkit covers most statutory, common law and professional requirements, as well as training, assurance processes and change control processes. From March 2016 the IG toolkit with be replaced by the NHS Digital Data Security and Protections Assurance Toolkit -however reporting will be similar for the practice.

Annual improvement plans will be developed each year to ensure the practice achieves a satisfactory level in all requirements. As the IGT and DS&P are publicly available assessments the scores of partner organisations will be used to assess their suitability to share information and to conduct business with.

The PRACTICE's progress will be reported to the Partners at regular intervals by the SIRO. Compliance with the IG Toolkit will provide assurance to the Partners that the majority of strategic information governance objectives are being met.

The practice will comply with the NHSD deadlines for submission of updates and final assessment.

IG Policies

The practice is committed to ensuring that its policies follow the HORUS model as proposed by the Department of Health to ensure compliance with legislation, including the GDPR 2016 and Data Protection Act 2018.

The principles of this model are that information is:

- Held safely and confidentially;
- Obtained fairly and lawfully;
- Recorded accurately and reliably;
- Used effectively and ethically;
- Shared and disclosed appropriately and lawfully.

To deliver this model, the practice will ensure that:

- policies and procedures are in place to facilitate compliance with all relevant legislation, regulations and duties;
- compliance with the Data Protection Act 2018 is maintained when handling Personal Confidential Data, except where there is a legal requirement to override the Act;
- information is appropriate for the purpose intended and that at all times the integrity of information is developed, monitored and maintained;
- information made available for operational purposes is maintained within set parameters relating to its importance via appropriate procedures and computer resilience systems;
- all identifiable information relating to patients is regarded as confidential;
- all identifiable information relating to staff is regarded as confidential, except where national policy on accountability and openness requires otherwise;
- when person identifiable data is shared, the sharing complies with the law;
- guidance and best practice and both service user rights and public interest are respected;
- non-confidential information relating to THE PRACTICE and its services is made available to the public through a variety of media, in line with the Freedom of Information Act and Environmental Information Regulations;
- will have clear procedures and arrangements for liaison with the press and broadcasting media;
- patients and service users will have access to information relating to their own health care, options and treatment and their rights as patients;
- undertake or commission annual audits of compliance with legal requirements;
- information and IT security, information quality and record management requirements are met in accordance with the DS&P Toolkit;
- the roles and responsibilities identified within the IG Framework are integrated and embedded within the organisation;
- procedures for the effective and secure management of its information assets and resources are established and maintained;
- information is managed throughout its lifecycle of creation, retention, maintenance, use and disposal;
- procedures for information quality assurance and the effective management of records are established and maintained;
- information is effectively managed so that it is accurate, up-to-date, secure, retrievable and available when required;
- incident reporting procedures, which includes the investigation of all reported instances of actual or potential breaches of confidentiality and security are established and maintained;

- Risk Management and reporting procedures are established and maintained, and will have in place risk controls and monitoring processes all reported information risks;
- relevant instruction and training is provided to all staff through induction and thereafter annually in relation to this policy.

IG Resources

The Information Governance Policy and Framework is enacted through the Information Governance Improvement Plan. This covers major elements of information governance implementation, including:

- Completion of the IG/DS&P Toolkit;
- Implementation of relevant policies and procedures;
- Information flow mapping;
- Information asset register and asset risk assessments;
- Incident reporting and management;
- Mandatory and specialist training;
- Annual assurance statements from IAOs to the SIRO, and onwards to the partners

The IGSG will identify any policy associated resource implications incurred by the implementation of the Information Governance improvement plan. Business cases will be developed to deliver specific initiatives of projects (if necessary).

Incident Reporting & Management

Incidents must be reported and managed through established processes. Significant issues will be subject to full investigation and reporting action. Incidents relating to personal information will be reported to the Caldicott Guardian whilst those of a more corporate nature will be reported to the SIRO.

THE PRACTICE will put in place suitable mechanisms to ensure staff identify and manage information risks in line with existing risk management policy and processes.

All information governance incidents must be reported as soon as they are detected in accordance with THE PRACTICE's Incident Reporting and Management procedure.

Information Security

With the increasing use of electronic data and ways of working which rely on the use of electronic information and communication systems to deliver services, there is a need for professional advice and guidance on their use as well as the need to ensure that they are maintained and operated to the required standards in a safe and secure environment.

Risk Management

The ability to apply good risk management principles to IG is fundamental and THE PRACTICE will apply them through organisational policies.

Risk assessment will also be included as part of the Information Asset Owners role. Any information flows from or in to identified information assets will be risk assessed and the results reported to the PRACTICE SIRO for risk mitigation, acceptance or transfer.

Legal Compliance

The Data Protection legislation (GDPR and DPA1998/2018) is the most fundamental piece of legislation that underpins Information Governance. The practice is registered with the Information Commissioners Office and will fully comply with all legal requirements of the law. A process will be adopted to ensure that a review of all of new systems is carried out and where requirements such as the need for Privacy Impact Assessments (PIA) are highlighted these will be completed. This will be included in the IG service specification.

Training and Staff Support

Fundamental to the success of delivering the Information Governance Policy is developing an Information Governance culture within the PRACTICE. Awareness and training will be provided to all staff that utilise information in their day-to-day work to promote this culture. In order to achieve this, the IGSG will ensure:

- all staff complete an Induction session when they first start employment which will include Information Governance. In subsequent years all staff are required to complete further Information Governance training as set out in the on-line IG Training Tool (IGTT). This is an annual exercise and is required to meet a satisfactory level within the IG Toolkit;
- specific modules available for the Caldicott Guardian, SIRO, IAOs and IG staff themselves are completed;
- all staff undertake an annual training needs analysis and any recommendations identified will be complied with by staff;
- keep all staff informed of compliance and standards set to support this policy via staff bulletins and where necessary Information Governance specific messages;
- implement staff surveys to assess levels of understanding and ensure staff are fully aware of their responsibilities;
- provide staff with the opportunity to develop more detailed knowledge and appreciation of the role of information governance through:

    - IG Policies and this policy;
    - Induction, mandatory and refresher training;
    - Line manager support;
    - Specific training courses for specialist roles.

Implementation & Dissemination

This policy once approved by the Partners will be shared with all members of staff. A team briefing will also be provided to support this dissemination.

The implementation of this IG policy and IG Toolkit improvement plan will ensure that information is more effectively managed in the PRACTICE. To support this policy, THE PRACTICE will implement key IG policies and will ensure that staff abide by these.

Each year the IG policy will be reviewed, and a revised DS&P Toolkit improvement plan will be developed against the IG Toolkit attainment levels and scores, thus identifying the key areas for a programme of continuous improvement.

Policy, Protocol and Procedure Distribution

All employee-based policies, protocols and procedures will be made available on the practice risk management system and will be highlighted in staff briefings. Knowledge of the key details of Information Governance related policies will be tested through the use of the online Information Governance training tool, and the use of staff surveys and/or confidentiality audits to test knowledge in particular areas.

Monitoring and Review

This policy will be reviewed on the first anniversary following its adoption and subsequently every two years until rescinded or superseded. An earlier review of this document may be undertaken in the event of:

- Legislative or case law changes;
- Changes or release of good practice or statutory guidance;
- Identified deficiencies, risks or following significant incidents reported;
- Changes to organisational infrastructure.
- New vulnerabilities;
- Practice change or change in system/technology;
- Changing methodology.

Performance Indicators

The Information Governance and DS&P Toolkit submission is a mandatory annual return; the criteria for compliance are set out within the relevant Toolkit. The successful implementation of Information Governance across the organisation will be reflected in the achievement level produced from the annual Toolkit submission.

Performance against this policy will be monitored against the IG Toolkit requirements by the IGSG, and escalated to the Partners. The level of assurance will be submitted officially via the Information Governance Toolkit on an annual basis.

Internal Reporting

Formal reporting will be managed through the IGSG. The Practice Manager will establish effective reporting arrangements with the partners to ensure the practice is receiving ongoing assurance of their IG performance and use these reports as an opportunity to quickly identify and escalate any issues or risks at an early stage.

Key Legislation & Guidance

This policy should be read in conjunction with the Information Governance Staff Handbook which outlines the procedures in relation to:

- Confidentiality and Data Protection
- Code of Conduct (in respect of confidentiality)
- IG Training
- Information Sharing
- Privacy Impact Assessments
- Information Security / Safe have procedures
- Information Risk assessment and Management Programme
- Records Management
- Subject Access Requests
- IG Incident Management
- Mobile Media / Social Networking
- Freedom of Information

Key legislation includes:

- Access to Health Records Act 1990
- Computer Misuse Act 1990
- Data Protection Act 1998/2018
- General Data Protection Regulation 2016
- Freedom of Information Act 2000
- Civil Contingencies Act 2004
- Health and Social Care Act 2012
- Fraud Act 2006
- NHS Act 2006

Further References (if not included above)

The following references can be accessed via the links provided:
• Data Protection Act 1998 available from www.**opsi**.go.uk
• Access to Health Records Act 1990 available from www.**opsi**.go.uk
• Human Rights Act 1998 available from www.**opsi**.go.uk
• Freedom of Information available from www.**opsi**.go.uk
• Environmental Information Regulations
http://www.ico.org.uk/for_organisations/environmental_information/guide
• Record Management available from
http://www.nationalarchives.gov.uk/information-management/projects-andwork/information-records-management.htm
• Common Law of Confidentiality
• NHS Confidentiality- code of practice available from
https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice
• Calidicott Report available from
https://www.gov.uk/government/publications/the-information-governance-review
• The Health and Social Care Act
http://www.legislation.gov.uk/ukdsi/2013/9780111533055
• Crime and Disorder Act 1998
http://www.legislation.gov.uk/ukpga/1998/37/contents
• Protection of Children Act 1999
http://www.legislation.gov.uk/ukpga/1999/14/contents

Equality and Diversity Statement

The organisation aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others.

All policies and procedures are developed in line with the PRACTICE's Equality and Diversity policies and need to take into account the diverse needs of the community that is served. The Equality Impact Assessment tool is designed to help consider the needs and assess the impact of the policy being developed.

The practice is committed to ensuring that it treats its employees fairly, equitably and reasonably and that it does not discriminate against individuals or groups on the basis of their ethnic origin, physical or mental abilities, gender, age, religious beliefs or sexual orientation.

APPENDIX 1

Red House Surgery

INFORMATION GOVERNANCE STEERING GROUP

TERMS OF REFERENCE

1.0 TITLE &FORMATION

Information Governance Steering Group (IGSG)

Formed:

2.0 STATUS & DELEGATED AUTHORITY

2.1 The Information Governance Steering Group is a formal committee of the (THE PRACTICE). The Group is authorised to make decisions which are:

(i) Within these Terms of Reference
(ii) Specifically referred by the partners

2.2 All procedural matters in respect of conduct of meetings shall follow the practice policy.

2.3 The Information Governance Steering Group is authorised by the partners to carry out any activity within its terms of reference. It is authorised to seek clarification and further investigation of any Information Governance (IG) related matter, and to request any relevant information from any employee.

2.4 The Information Governance Steering Group is authorised by the partners to obtain outside or other independent professional advice with relevant experience and expertise if required.

2.5 The Group may recommend actions which require financial expenditure but the Group itself does not have any delegated powers of expenditure, as this rests with the relevant budget holder.

2.6 The Group may establish such working groups or project teams as it considers appropriate to support its objectives and duties. Any group or project team so established shall have terms of reference, including reporting arrangements, approved by the Information Governance Steering Group.

3.0 OBJECTIVES

3.1 The overall objective of the Group is to:

Ensure that there are effective strategies, structures, policies and systems in place to meet the Information Governance Requirements and Agenda.

Information Governance is defined as a framework for handling personal and corporate information in a confidential and secure manner to appropriate ethical and quality standards in a modern health service.

3.2 In fulfilling the objective under 3.1 above, the Group shall:

(i) be mindful of the principles of integrated governance and where necessary identify, consider and communicate risks and impacts that may extend to the wider organisation and which arise through the exercise of its delegated functions.

(ii) link its programme of work to the strategic objectives of the practice

12 **4.0 ACCOUNTABILITY**

4.1 The Information Governance Steering Group is accountable to the Partners

4.2 The nominated Senior Information Risk Owner (SIRO) will act as an advocate for information risk in internal discussions. The SIRO is responsible for providing written advice to the Senior Partners on the content of the Annual Governance Statement (AGS) in regard to information risk.

4.3 The Information Asset Owners' role is to understand and address risks to the information assets they 'own'; and to provide assurance to the SIRO on the security and use of these assets.

13 **5.0 MEMBERSHIP &ATTENDANCE**

5.2 Full members (with voting rights):

- Senior Information Risk Owner (SIRO)
- Caldicott Guardian
- General Manager
-

5.3 The Group will be chaired by the Senior Information Risk Owner (SIRO). The Vice Chair will be the Caldicott Guardian

5.4 Additional members with specific expertise may be co-opted to the Group as required.

5.5 Members shall be assumed to be attending a meeting of the Group unless apologies are sent in advance to the secretary. If a full member cannot attend and if reasonably possible, they should appoint a suitably briefed deputy to attend on their behalf. Deputies shall contribute to the quorum and shall have voting rights as per full members.

5.6 The Practice Manager shall ensure that arrangements are in place for the provision of administrative support to the Group.

6.1 DUTIES

The duties of the Group are to:

- Work on behalf of the Partners to ensure the practice complies with the Information Governance and record-keeping elements of national standards and criteria including:

- Information Governance Toolkit Standards
- NHS Litigation Authority Risk Management Standards
- Care Quality Commission Standards
- NHS Operating Framework
- Develop action plans to ensure compliance with these standards.
- Seek assurance around compliance and completed recommendations

- Establish an Information Governance improvement plan to secure the necessary implementation of resources and monitor the implementation of that action plan.

- To review and approve Practice Information Governance policies on behalf of the Partners

- Consider serious breaches of confidentiality and information security and where appropriate undertake or recommend remedial action.

- To review the analysis and management of Information Governance incidents and prevented incidents to ensure that any quality issues have been identified and remedial actions taken to protect patients and the organisation and that any lessons learnt;

    - Are communicated throughout the organisation
    - Are used to review local processes and structures to enhance information governance

- To review and promote Information Risk awareness and control

- Consider and monitor the implementation of recommendations made in relevant internal audit reports or other sources of assurance.

- Promote and monitor service user feedback with regard to Information Governance issues.

- Identifying training needs, agreeing on delivery method and monitoring progress.

- Set the strategic guidelines for sharing information with external organisations.

- Consider any relevant issues arising from practice policy and national guidance and to also consider the impact (including risks and resource requirements) of stated forthcoming government policy and legislation.

- Monitor and review the policy, policy and guidance for the management of records in the practice.

- Ensure that the practice, through its service areas, implements the Records Management policy (and other related policies) and provides guidance on the development and review of local systems.

- Approve standards for the format and quality of all records including writing and content.

7.0 MEETINGS

7.1 The Group will meet every 6 months unless otherwise agreed by the Chair.

7.2 The Chair of the Group may also convene special meetings.

7.3 Venues will be agreed and notified to members and as relevant, to co- opted members and observers.

7.4 The Group shall devise an annual "business cycle" which identifies the dates of meetings and the matters which are to be considered at each meeting.

8.0 QUORUM

8.1 The quorum will be two members which must include the Chair or Vice Chair.

9.0 DECISION MAKING

9.1 The Group has joint and collective responsibility for agreeing decisions.

Decisions shall be reached by consensus where possible, and where there is not unanimous agreement, a vote shall be taken and the result recorded. The Chair shall have casting vote where applicable.

9.2 Para 9.1 above notwithstanding, in the event agreement cannot be reached on a particular issue, the Chair may opt to refer a matter to the Partners for decision.

9.3 Co-opted members and observers do not have voting rights.

9.4 In the event of an urgent decision being required between meetings on any matter within the Terms of Reference of the Group, the Chair may take 'Chair's Action'. The action will be reported to the next meeting for ratification and recorded in the minutes/notes.

10.0 PAPERS

10.1 The agenda for each meeting will be devised by the Practice Manager and agreed with the Chair.

10.2 The deadline for agenda items will be communicated prior to each meeting, with any urgent business beyond the deadline to be agreed with the Chair in advance of the meeting.

10.3 The agenda and associated papers/documents for each meeting will be distributed in advance of the meeting to all members and co-opted members.

10.4 Members have responsibility to manage the papers/documents in accordance with the Practice's Records Management policy.

10.5 Draft Minutes/notes of each meeting will agreed by the Chair before distribution to the members.

10.6 At the discretion of the Chair, matters of a confidential or sensitive nature concerning information which may be exempt from disclosure under the Freedom of Information Act may be covered under a "Part 2" meeting of the Group. If a "Part 2" meeting is held, the following shall apply:

(i) The Chair shall have the power to exclude any full members of the group from the meeting provided that there are at least two members other than the Chair present.

(ii) Unless determined otherwise by the Chair, papers &minutes of a Part 2 meeting shall be circulated to those attending only.

(iii) In the event of a request made under the Freedom of Information Act which is pertinent to Part 2 Group papers, a decision on exemption from disclosure shall be made by the Chair in consultation with the Data Protection Officer. Formal legal advice shall be obtained if considered appropriate.

11. REPORTING

11.1 The minutes of Group meetings shall be formally recorded and submitted to the Partners.

11.2 Copies of the approved agenda and minutes submitted for the Group will be published on the practice intranet. (Unless they contain personal or other sensitive information exempt from disclosure under the Freedom of Information Act).

12.0 TERMS OF REFERENCE – RATIFICATION AND REVIEW

12.1 The Terms of Reference will be agreed by the Group and ratified by the Partners.

12.2 The Terms of Reference will be reviewed annually or earlier at the Chair's discretion.

13.0 DISSOLUTION

13.1 The Group may only be dissolved with the agreement of the Partners or by default in the event of the Practice ceasing to exist as an independent, statutory body.

Date: October 2018