Information Risk and Security Policy

Document No.	WHC 08:09	Version No.	1.1
Approved by	(old) Policies and Procedures Group	Date Approved	6/8/19
Ratified by	IG POG	Date Ratified	1.0 - 13/2/20
Minor amendment – updated references to additional info/SOPs and sections 5.3; 5.4; 5.5 on IAO/IAA roles and WHC Infogov function.	IG POG	Date Approved	1.1 - 16/11/20
Ratified by	Policies and Procedures Group	Date Ratified	17/11/20
Date Implemented	1.0 - 13/2/20 1.1 – 27/11/20	Next Review Date	August 2022
Status		RATIFIED	
Target Audience (who does the document apply to and who should be using it)		Wiltshire Health and Care staff	
Accountable Director		Managing Director	
Policy Author/Originator – **Any comments on this document should, in the first instance, be addressed to whc.policyqueries@nhs.net**		Business Manager	
If developed in partnership with another agency, ratification details of the relevant agency		Adapted from Salisbury Foundation Trust (SFT)'s policy	

Equality Impact and Parity of Esteem

Wiltshire Health and Care staff strive to ensure equality of opportunity and parity of esteem for all service users, local people and the workforce. As an employer and a provider of health care, we aim to ensure that none are placed at a disadvantage as a result of its policies and procedures. This document has therefore been equality impact assessed in line with current legislation to ensure fairness and consistency for all those covered by it regardless of their individuality. This means all our services are accessible, appropriate and sensitive to the needs of the individual.

References: ***NHS England 'Everyone Counts: planning for patients 2014-15 / 2018-19' and The Mental Health Crisis Care Concordat (DH 2014).***

Safeguarding

Wiltshire Health and Care have a strong commitment to care that is safe, of a high quality and that upholds our patients' rights. All our patients have the right to live lives free from abuse or neglect and, where they are able to, to make or be supported to make informed decisions and choices about their treatment, care and support. Where patients are not able to make their own decisions, Wiltshire Health and Care staff are committed to ensuring that treatment, care and support is undertaken in accordance with the person's best interests. In order to fulfil these commitments, Wiltshire Health and Care follow the Safeguarding principles and responsibilities laid out in sections 42-46 of the Care Act (2014) and are informed by, and apply, the guiding principles and provisions of the Mental Capacity Act (2005) (refer to Wiltshire Health and Care Safeguarding Adults Policy and Procedure, and Mental Capacity Act Policy and Procedure).
Regarding children, WHC is responsible for providing services in accordance with Section 11 of the Children's Act (1989) and works under the principles of Working Together to Safeguard Children (2018).

Special Cases

There are no special cases.

CONTENTS

1. Policy Purpose

The Information Risk & Security Policy has been created to:

- Protect WHC, its staff and its patients from information risks where the likelihood of occurrence and the consequences are significant
- Provide a consistent risk management framework in which information risks will be identified, considered and addressed in key approval, review and control processes
- Encourage proactive rather than reactive risk management
- Provide assistance to and improve the quality of decision making throughout WHC
- Meet legal or statutory requirements
- Assist in safeguarding WHC's information assets
- Avoid unnecessary impacts on day to day business
- Define the responsibilities of key stakeholders

2. Regulatory/Legal Framework

The policy is required by the NHS Chief Executive (see Ref: 3, recommendation 4), based on the Government's Data Handling Review Report (Ref: 4, paragraphs 2.21, 2.33).

2.1 Further Reading and Links to Other Policies

The following is a list of other policies, procedural documents or guidance documents (internal or external) to which employees should refer for further details:

Ref. No.	Document Title	Document Location
1	Information Governance Policy and Strategic Management Framework	W\Wiltshire Health and Care Documents
2	Information Asset Owner/Information Asset Administrator Handbook	W\Wiltshire Health and Care Documents
3	SOP Information Asset Register process	W\Wiltshire Health and Care Documents
4	SOP IG Incident Reporting and Response	W\Wiltshire Health and Care Documents
5	Risk management Strategy & Framework (general strategy/framework, not just related to Information Security and Risk)	W\Wiltshire Health and Care Documents
6	Incident Management Policy (general policy, not just related to Information Incidents)	W\Wiltshire Health and Care Documents
7	SOP Serious Incident Investigation (general guidance, not just related to Information Incidents)	W\Wiltshire Health and Care Documents
8	Management of Contracts/SLAs	W\Wiltshire Health and Care Documents
9	Data Security & Protection Toolkit	www.dsptoolkit.nhs.uk
10	Care Cert cyber security incident reporting template	W\Wiltshire Health and Care Documents

3. Document Details

3.1 Introduction and Purpose of the Document

Wiltshire Health and Care (WHC), places great importance on minimising any possible or potential risk to information security whilst safeguarding the interests of patients and staff, as well as protecting the position of WHC itself. To achieve this, Information Security Risk Management must be implemented and embedded into the key controls and approval processes of all major business processes and functions of WHC.

Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in Clinical Governance, service planning and performance management.

Information risk is inherent in all administrative and business activities; everyone working for or on behalf of WHC continuously manages information risk. The aim of Information Risk Management is not to eliminate risk, but rather to provide the structural means to identify, prioritise, and manage the risks involved in all WHC activities. This involves a balance between the cost of managing and treating information risks against the anticipated benefits that will be derived.

WHC acknowledges that information risk and security management is an essential element of broader information governance and an integral part of good management practice. The intent is to embed information risk management in a very practical way into business processes and functions – such as through key approval and review processes / controls – rather than imposing it as an extra requirement.

Information risk management is integrated into WHC's overall corporate risk management process, reporting and monitoring risk and incidents through the same set of mechanisms.

4. Main Policy Content Details

4.1 Scope

This policy covers all information systems purchased, developed and managed by, or on behalf of, WHC and any individual, directly or otherwise employed by the organisation. This policy is applicable to all areas of WHC and adherence should be included in all contracts for outsourced or shared services. There are no exclusions. (Ref 8)

4.2 Information Risk Definitions

Key definitions are:

- **Risk -**The chance of something happening, which will have an impact upon objectives. It is measured in terms of consequence and likelihood.

- **Consequence -** The outcome of an event or situation, expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event.

- **Likelihood -** A qualitative description or synonym for probability or frequency.

- **Risk Assessment -** The overall process of risk analysis and risk evaluation.

- **Risk Management -** The culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects.

- **Risk Treatment -** Selection and implementation of appropriate options for dealing with risk. Conceptually, treatment options will involve one or a combination of the following five strategies:

    - Avoid the risk
    - Reduce the likelihood of occurrence
    - Reduce the consequences of occurrence
    - Transfer the risk
    - Retain/accept the risk

- **Risk Management Process -** The systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying and analysing, evaluating, treating, monitoring and communicating risk.

- **Information Security Incident Management –** Incident management is a programme which defines and implements a process that an organisation may adopt, to promote its own welfare, the security of information and the security of the public.

  There are three basic types of events:

A. **A normal event** does not affect critical components, or require change controls, prior to the implementation of a resolution. Normal events do not require the participation of senior personnel or management notification of the event.

B. **An escalated event** affects critical production systems, or requires the implementation of a resolution that must follow a change control process. Escalated events require the participation of senior personnel and stakeholder notification of the event.

C. **An emergency** is an event which may;

- impact the health or safety of human beings
- breach primary controls of critical systems
- materially affect component performance or, because of impact to component systems, prevent activities which protect or may affect the health or safety of individuals
- be deemed an emergency as a matter of policy or by declaration by the available incident coordinator.

4.3 Security Incident Management

Any incident involving the actual or potential loss of personal or sensitive data, or corporate information that could lead to distress, identity fraud or have other significant impact on individuals must be considered as serious. Any such incidence should be reported by raising a DATIX Incident report; this will be notified via DATIX to the Corporate Services Team.

A Standard Operating Procedure (SOP) IG Incident Reporting and Response is available on the Master Documents Tracker to guide staff through the process of reporting and investigating losses of data or IT items.

4.4 Reporting data losses to the ICO

It is the responsibility of the Managing Director and SIRO (or their delegate) to report data security breaches to the ICO, Commissioning Authority and the Department of Health and Social Care. Security breaches must be reported to the ICO using their online reporting tool.

4.5 NHS Digital Cyber Security Programme- CareCERT Project

NHS Digital (formerly the Health and Social Care Information Centre (HSCIC)) has been commissioned by the Department of Health and Social Care to provide a Care Computer Emergency Response Team (CareCERT). CareCERT will offer advice and guidance to support health and social care organisations to respond effectively and safely to cyber security threats. The service will enable a coordinated approach to be taken by informing organisations about cyber security vulnerabilities, mitigating risks, and reacting to cyber security threats and attacks.

When a CareCERT Cyber Security alert is issued this will be considered by WHC's Informatics/IG team, in liaison with its suppliers, to determine whether there is a potential impact to WHC, the level of risk involved, and the actions required to be taken.

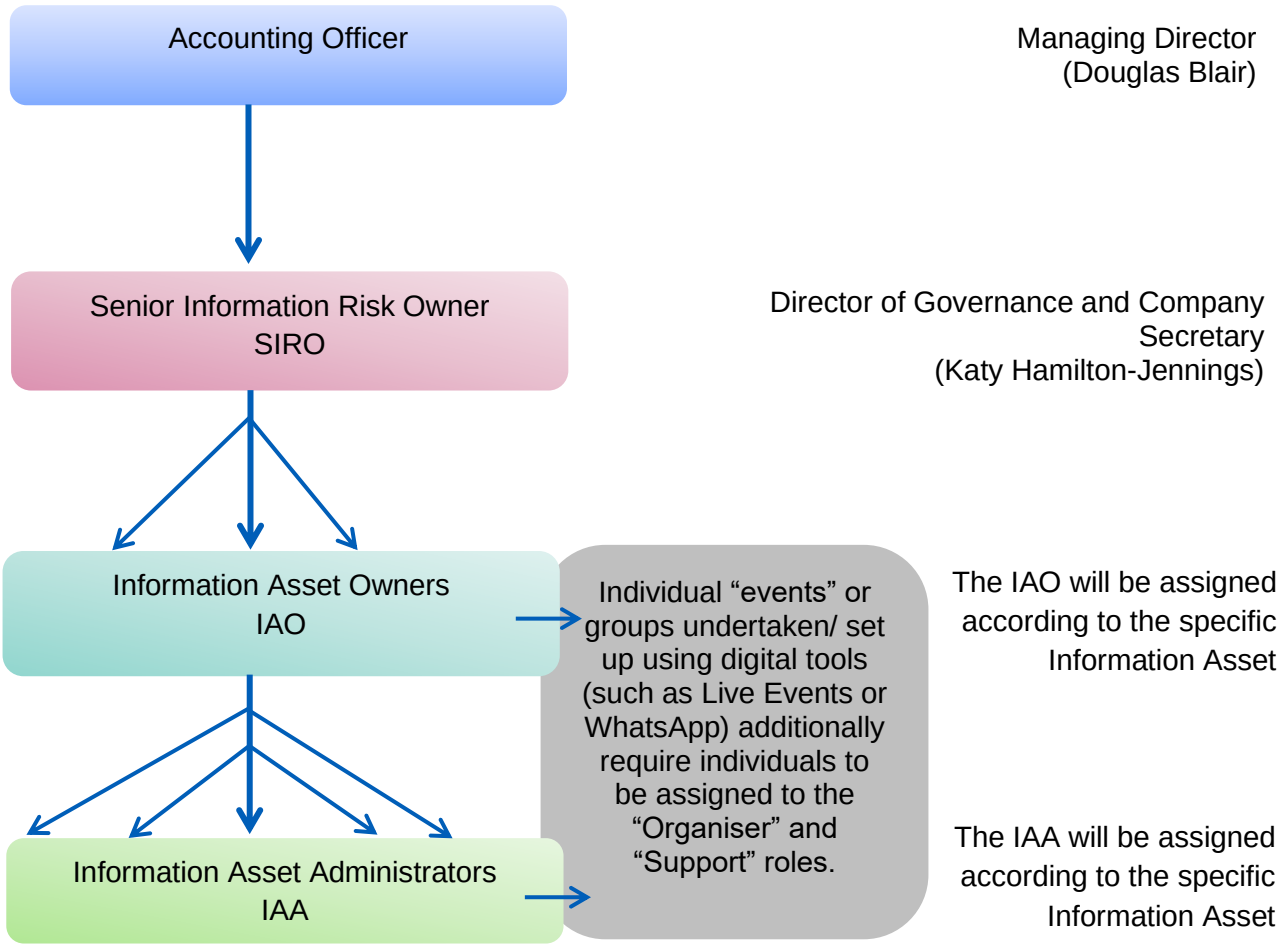
In the case of severe threats, the SIRO and other WHC Board Members will be immediately informed in line with the processes detailed in Section 6.

A log of the CareCERT Cyber Security alerts will be maintained by our IT Service Provider detailing the risks, actions to be taken and progress. A copy of the log format is linked on the Master Documents Tracker (Ref 10). This will be used as a basis for regular reports to the Information Governance Policy & Oversight Group (IG POG) and for monitoring purposes.

4.6 Data Privacy Impact Assessment (DPIA)

No amendment has been made to the methods by which personal data is processed by WHC and therefore it is the opinion of the Senior Information Risk Owner that a DPIA is not required for this policy.

5. Duties and Responsibilities of Individuals and Groups



5.1 Managing Director

The Managing Director is ultimately responsible for the implementation of this document.

WHC's Managing Director as Accountable Officer has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level. They are also accountable to the Department of Health and Social Care, NHS Digital, NHS Improvement, and the Information Commissioners' Office for information security breaches.

5.2 Senior Information Risk Owner (SIRO)

The SIRO is responsible for coordinating the development and maintenance of information security and risk management policies, procedures and standards for WHC. This includes responsibility for the on-going development and day-to-day management of the WHC's Risk Management Programme for information privacy and security.

The SIRO is to advise the Managing Director and WHC Board on information security and risk management strategies and provide periodic reports and briefings on progress.

The SIRO is to ensure that Information Assets are identified (Ref 3) that a register of assets is maintained, and that each asset has an assigned Information Asset Owner.

5.3 Information Asset Owner (IAO)

The IAO documents, understands and monitors the information asset and its use and security of information held within the IA. The IAO assigns an Information Asset Administrator (IAA) to each IA.

IAOs ensure that information risk assessments are performed annually on all information assets for which they have been assigned 'ownership'. This forms part of the audit report which is completed by the IAA annually and signed off by the IAO. The IAO will submit the audit report including risk assessment results and associated mitigation plans to whc.informationgovernance@nhs.net for the SIRO to review. This will include mitigation plans and specific actions with expected completion dates, as well as an account of residual risks.

A description of the IAO role and responsibilities is contained in the IAO and IAA handbook (Ref 2), which forms part of IAO/IAA training. This is found on the intranet:
https://nww.connected.wiltshirehealthcare.nhs.uk/support-services/corporate-services/information-governance/information-asset-register-and-roles-and-responsibilities/

5.4 Information Asset Administrator (IAA)

The IAA provides support to the IAO:

- to ensure that WHC policies and procedures are followed
- to recognise and report potential security risks or actual security incidents via DATIX
- to manage incidents
- to maintain users' log and associated records about the information asset
- to ensure that the information asset register is kept up to date with the asset information
- to complete the annual audit report (including risk assessment)

A description of the IAA role and responsibilities is contained in the IAO and IAA handbook (Ref 2), which forms part of IAO/IAA training. This is found on the intranet
https://nww.connected.wiltshirehealthcare.nhs.uk/support-services/corporate-services/information-governance/information-asset-register-and-roles-and-responsibilities/

5.5 Information Governance function

The IG function is responsible for:

- Reporting all security of information incidents into the DSPT. (Incidents should be raised by individuals and/or via DATIX as soon as possible in accordance with the SOP IG Incident Reporting and Response – Ref 4).
- Reporting, (where directed by DSPT) serious incidents to the Information Commissioner's Office, and comply with requests from them for further information to support investigations.

- Providing IG training and supporting documentation including; IGIT training, IAA/IAO training
- Providing compliance tracker reports to the Information Governance Policy & Oversight Group (IG POG) detailing departmental (IAO) compliance levels, which highlight areas of good practice and of concern;
- Providing information risk, security and specialist advice, support and guidance to the IAOs and IAAs;
- Cascading emails to the IAOs and IAAs highlighting key changes to impacting legislation, Department of Health and Social Care guidance, policies or procedures, which require alterations or amendments to systems or procedures;
- Providing feedback to the IAOs on their department and IAAs' levels of compliance;
- Reviewing and validating the quality and content of the evidence submitted by the IAOs;
- Investigating and reporting serious Incidents on behalf of the SIRO and WHC Board;
- Producing an annual Information Security Assurance Compliance Report for the WHC Board.

5.6 Ward/Service Managers, and Managers for Non Clinical Services

All Ward/Service Managers and Managers for Non Clinical Services are to ensure that the list of new or revised policies, competencies, clinical guidelines, strategies, plans, protocols or procedural documents published each month is on the agenda at meetings to ensure that the documents are drawn to the attention of managers and general users. All Ward/Service Managers and Managers for Non Clinical Services must ensure that employees within their area are aware of the document; able to implement the document and that any superseded documents are destroyed.

5.7 Document Author

The document author is responsible for identifying the need for a change in this document as a result of becoming aware of changes in practice, changes to statutory requirements, revised professional or clinical standards and local/national directives, and resubmitting the document for approval and republication if changes are required.

5.8 Target Audience – as indicated on the Cover Page of this document

The target audience has the responsibility to ensure their compliance with this document by:

- Ensuring any training required is attended and kept up to date.
- Ensuring any competencies required are maintained.
- Co-operating with the development and implementation of policies as part of their normal duties and responsibilities.

6. Monitoring Compliance and Effectiveness of Implementation

The arrangements for monitoring compliance are outlined in the table below:-

Measurable policy objectives	Monitoring / audit method	Monitoring responsibility (individual/group /committee)	Lead	Frequency of monitoring	Reporting arrangements (committee / group to which monitoring results are presented)	What action will be taken if gaps are identified?
Review and report on the number of information security breaches/incidents and compare with previous periods. These include those reportable to ICO.	Tracking/reporting via DATIX reports or as reported by individuals	IG function within Corporate Services	JPF (Business Manager	Constant monitoring via automated reports from DATIX. Quarterly reports to IGPOG	Information Governance Policy & Oversight Group (IG POG)	Staff training or, depending on severity, implementation of HR conduct management.
Review and report on the number/type of CareCert alerts	Tracked on spreadsheet	Contracted IT Service Provider	KS (Head of IT)	Quarterly	IT service provider will report to Head of IT; report will go to IG POG	Investigation into IT systems
Content of Information Asset Register (IAR)	Tracking/updating with staff or role changes	IG function within Corporate Services	AB - BSO (Corporate Services)	Bi-annual	Bi-annual report to IG POG in preparation for bi-annual Data Security & Protection Toolkit submissions	Review of IG function priorities
Monitor Risk Assessments within IAR	Tracking/updating of IAR	IG function within Corporate Services	IG function (Corporate Services)	Monthly review	Quarterly formal report to IG POG	IG POG Action Tracker
Assurance Compliance Report on DSPT.	Tracked on spreadsheet	IG function within Corporate Services	JPF – Business Manager	Quarterly review to IGPOG	Annually formal report to IG POG	Ongoing DSPT actions
Identified IAO and IAA review	IAA Report Template and IAO/IAA handbook	IG function within Corporate Services/SIRO	IG function (Corporate Services)/ SIRO- KHJ	Quarterly	IG POG	

7. Review Date and Consultation Process

7.1 Review Date

This document will be fully reviewed every 3 years (or after 1 year for new documents) in accordance with the Wiltshire Health and Care agreed process for reviewing its documents. Changes in practice, to statutory requirements, revised professional or clinical standards and/or local/national directives are to be made as and when the change is identified.

7.2 Consultation Process

The following is a list of consultees in formulating this document and the date that they approved the document:

Job Title / Department	Date Consultee Agreed Document Contents
Senior Information Risk Owner	Sent by e 25/6/19 – comments incorporated into 0.3
Data Protection Officer	
Head of IT	Sent by e 25/6/19 – comments incorporated into 0.3
IT Project Manager	Sent 8/8/19 – no comments
Risk & Complaints Manager	Sent 8/8/19 – no comments
Quality Governance System Analyst	8/8/19
Corporate Services Project Manager	28/10/20 – revised to align with IAR documentation

Appendix A – Equality Impact Assessment

The policy should have no impact on those with protected characteristics, but the following summarises the organisation's general framework:

Protected Characteristic	For employees	For patients
Age	Employment practices including recruitment, personal development, promotion, entitlements and retention encompass employees with protected characteristics.	• Services are provided, regardless of age, on the basis of clinical need alone. •
Disability -	Reasonable steps will be taken to accommodate the disabled person's requirements, including: • Physical access • Format of information • Time of interview or consultation event • Personal assistance • Interpreter • Induction loop system • Independent living equipment • Content of interview of course etc.	Reasonable steps are taken to accommodate the disabled person's requirements, including: • Physical access • Format of information • Time of consultation /event • Personal assistance • Interpreter • Induction loop system
Gender reassignment -	There is equal access to recruitment, personal development, promotion and retention. Confidentiality about an individual's gender status is maintained.	There is equality of opportunity in relation to health care for individuals irrespective of whether they are male or female. Confidentiality about an individual's gender status is maintained and supported by a specific policy.
Marriage and Civil Partnership	There is equal access to recruitment, personal development, promotion and retention for individuals irrespective of whether they are single, divorced, separated, living together or married or in a civil partnership	There is equality of opportunity in relation to health care for individuals irrespective of whether they are single, divorced, separated, living together or married or in a civil partnership.
Pregnancy and Maternity -	There is equal access to recruitment, personal development, promotion and retention for female employees who are pregnant or on maternity leave. A woman is protected against discrimination on the grounds of pregnancy and maternity. With regard to employment, the woman is protected during the period of her pregnancy and any statutory maternity leave to which she is entitled. • There is a Flexible Working Policy.	There is equality of opportunity in relation to health care for women irrespective of whether they are pregnant or on maternity leave. A woman is protected against discrimination on the grounds of pregnancy and maternity.

Race - including Nationality and Ethnicity	There is provision for interpreter services for people whose first language is not English. Documents can be made available in alternative languages/formats Written communications are in plain English and the use of language particularly jargon or colloquialisms are avoided. Religion, belief and culture is respected.	There is provision for interpreter services for people whose first language is not English. Documents can be made available in alternative languages/formats Written communications are in plain English and the use of language particularly jargon or a colloquialism is avoided. Religion, belief and culture are respected.
Religion or Belief	HR policies cover consideration of: • Prayer facilities • Dietary requirements. • Gender of staff when caring for patients of opposite sex. • Respect for requests from staff to have time off for religious festivals and strategies. • Respect for dress codes	Equality and Diversity guidelines enable consideration of: • Prayer facilities • Dietary requirements. • Gender of staff when caring for patients of opposite sex. • Respect for religious festivals • Respect for dress codes
Sex	HR policies cover consideration of: • Equal access to recruitment, personal development, promotion and retention. • Childcare arrangements that do not exclude a candidate from employment and the need for flexible working. • The provision of single sex facilities, toilets	Single sex facilities, including toilets and on wards, are provided.
Sexual orientation	HR policies cover consideration of: • Recognition and respect of individual's sexuality. • Recognition of same sex relationships in respect of consent to care and treatment. • The maintenance of confidentiality about an individual's sexuality. • Consider the effect on heterosexual, gay, lesbian and bi-sexual people	There is: • Recognition and respect of individual's sexuality. • Recognition of same sex relationships in respect to consent. • The maintenance of confidentiality about an individual's sexuality. • Consideration of the effect on heterosexual, gay, lesbian and bi-sexual people

Appendix B – Quality Impact Assessment

Purpose To assess the impact of individual policies and procedural documents on the quality of care provided to patients by Wiltshire Health and Care		
Process The impact assessment is to be completed by the document author. In the case of clinical policies and documents, this should be in consultation with Clinical Leads and other relevant clinician representatives. Risks identified from the quality impact assessment must be specified on this form and the reasons for acceptance of those risks or mitigation measures explained.		
Monitoring the Level of Risk The mitigating actions and level of risk should be monitored by the author of the policy or procedural document or such other specified person. High Risks must be reported to the relevant Executive Lead.		
Impact Assessment Please explain or describe as applicable.		
1.	Consider the impact that your document will have on our ability to deliver high quality care.	*The policy will have no direct impact on the delivery of high quality care, but sets out the guidance to staff on how to maintain security of information, and what to do in the event that information is breached or lost.*
2.	The impact might be positive (an improvement) or negative (a risk to our ability to deliver high quality care).	
3.	Consider the overall service - for example: compromise in one area may be mitigated by higher standard of care overall.	*This document will not compromise care in any other area*
4.	Where you identify a risk, you must include identify the mitigating actions you will put in place. Specify who the lead for this risk is.	
Impact on Clinical Effectiveness & Patient Safety		
5.	Describe the impact of the document on clinical effectiveness. Consider issues such as our ability to deliver safe care; our ability to deliver effective care; and our ability to prevent avoidable harm.	*The policy will have no direct impact on clinical effectiveness and patient safety but, by following its guidance, information security breaches may be avoided.*

Impact on Patient & Carer Experience		
6.	Describe the impact of the policy or procedural document on patient / carer experience. Consider issues such as our ability to treat patients with dignity and respect; our ability to deliver an efficient service; our ability to deliver personalised care; and our ability to care for patients in an appropriate physical environment.	*The policy will have no direct impact on patient or carer experience but will provide assurance to patients/carers that we take our responsibilities for information security seriously.*
Impact on Inequalities, and Parity of Esteem		
7.	Describe the impact of the document on inequalities in our community. Consider whether the document will have a differential impact on certain groups of patients (such as those with a hearing impairment or those where English is not their first language).	*There should be no negative impact on any groups of patients.*