

## Information Governance Policy

The key messages the reader should note about this document are:

1. Sets out Information Governance Policy for the Trust, aligned to the new EU General Data Protection Regulation
2. Defines the Trust's Information Governance Framework, as required by the Data Security & Protection Toolkit
3. Over-arches the development of underlying IG procedures within the Trust
4. Gives the Information Governance team a mandate for its work
5. Encourages best practice aligned to data protection and other relevant law and NHS policy

## DOCUMENT SUMMARY SHEET

ALL sections of this form must be completed.

<b>1.1 Document title</b>	Information Governance Policy
<b>Document Reference Number</b>	IG-0001
<b>Key searchable words</b>	<i>Information Governance, Data Protection, Freedom of Information</i>
<b>Executive Team member responsible (title)</b>	Chief Financial Officer
<b>Document author (name and title)</b>	Carl Starbuck Information & Knowledge Manager
<b>Approved by (Committee/Group)</b>	Information Governance Group
<b>Date approved</b>	26/04/2018
<b>Ratified by</b>	Policy and Procedure Group
<b>Date ratified</b>	29 August 2018
<b>Review date</b>	29 August 2021
<b>Frequency of review</b>	<i>At least every three years</i>

### Amendment detail

Version	Amendment	Reason
0.1	This is a revision of an existing procedure	This is the first re-draft under the revised NHSLA standard format.
0.2	Minor amendments throughout	After Board review, 27 <sup>th</sup> November 2008
1.0	Ratified	Ratified IM&T, 23 <sup>rd</sup> January 2009
1.1	Minor updates to reflect toolkit changes & to feature "IG Framework" terminology.	First review, to reflect IGT v8.
2.0	Ratified	Ratified by Board of Directors
2.1	Changes to key contacts, general review and update, logo change.	Annual review by Carl Starbuck – Information & Knowledge Manager
3.0	Ratified	Ratified by Board of Directors
3.1	Updated to current template, modernisation of language and governance structures, inclusion of Caldicott 2 commitment to information sharing	Annual review by Carl Starbuck – Information & Knowledge Manager
4.0	Ratified	Ratified 14 <sup>th</sup> August 2014 – confirmed by SIRO. Caldicott Guardian & CIO present at approving meeting
	Review date extended	Executive Team agreed (1 December 2015) to extend the review date of this document from 9 October 2014 to 31 May 2016.
	Review date extended	31/5/17 Policy and Procedure Group agreed to extend from 1/9/17 to 25/5/18
4.1	Review and update	Transferred to current procedural document format (2018), refreshed for compliance with the General Data Protection Regulation and checked overall for currency & consistency by Carl Starbuck – Information & Knowledge Manager.
5.0	Ratified	Ratified at Policy and Procedure Group – 29 August 2018

<b>CONTENTS</b>		
<b>Section</b>	<b>Description</b>	<b>Page</b>
1	The Policy	5
	1.1 Flow chart of procedure (if relevant)	N/A
	1.2 Executive Summary	
	1.3 Description & Purpose of Policy	
	1.4 Scope	
	1.5 Openness	
	1.6 Information Security	
	1.7 Information Quality Assurance	
	1.8 Related Procedural Documents	
	1.9 Legal / Ethical Context	
	1.10 Year-On-Year Improvement / Maintenance Plan and Assessment	
	1.11 Information Governance Group	
	1.12 Duties and Responsibilities	
	1.13 Training	
2	Appendices included as relevant (include Appendices or a link to the relevant documents on staffnet)	N/A

## 1. The Policy

### 1.1 Flowchart of Policy (if relevant)

Not relevant for this policy.

### 1.2 Executive Summary

Information Governance is the legal and ethical framework under which Personal Confidential Data and otherwise confidential information is processed. It includes our approach to data quality, information security, confidentiality, information sharing and information retention and disposal. It gives assurance to the Trust and to stakeholders that personal information is dealt with lawfully, ethically, securely, efficiently and effectively, in order to deliver the best possible care whilst respecting the confidentiality of data subjects.

The Trust will establish and maintain policies and procedures to ensure compliance the Data Protection Act and the UK enactment of the EU General Data Protection Regulation, Computer Misuse Act, Freedom of Information Act, NHS Confidentiality Code of Practice, NHS Digital Data Security & Protection Toolkit and any other relevant legislation, directive or requirement issued by an appropriate body.

The scope of compliance is not limited to clinical information. It covers all information both of personal and sensitive / special category nature and that which is deemed to be commercially or business confidential.

### 1.3 Description & Purpose of Policy

This policy forms part of the Trust approach to Information Governance and establishes the Information Governance Framework. It will over-arch relevant procedural documentation in this area, mirroring legislation and regulatory requirements.

The purpose of this document is to set out the Trust Information Governance Policy and Framework, and empower the Information Governance team with a Board-level mandate for their continued work. It will over-arch numerous procedural documents that will underpin the required actions to improve and maintain the Trust Information Governance position, by progressing the requirements of the NHS Digital Data Security & Protection Toolkit and actions against other demands placed on the Trust in the context of the evolving national Information Governance agenda.

The Policy aims to encourage the uptake of IG best practice and observance of the requirements of appropriate legislation such that IG incidents are lessened or eradicated, with these ultimate key aims:

- Personal Confidential Data relating to service users, staff, FT membership and other individuals is handled in appropriate manner.
- Corporate information is handled according to appropriate consideration of the balance between commercial confidentiality, the need for openness, and the requirements of the Freedom of Information Act.
- The Trust is protected from harm to its reputation and punitive sanctions imposed by the Information Commissioners Office or other regulatory body.
- The Trust IG team continue to monitor the changing IG agenda and report important developments via the IG Group and upwards to the Executive Team and Trust Board.
- Performance against the NHS Digital Data Security & Protection Toolkit, appropriate CQC standards and other relevant IG initiatives will be closely monitored and championed so that Trust performance is improved, maintained and appropriately reported.
- That Trust staff in all areas, specialisations and roles are mindful of their obligations and best practice in the handling of Personal Confidential Data, and that they are adequately supported in their work by a highly developed and embedded IG Framework.
- That service users and other stakeholders are justifiably assured of the technical, systemic, operational and procedural measures in place to protect their information, maintain its confidentiality and use it appropriately to facilitate quality care and wider Trust business.
- That relevant information will be shared with partner organisations when it is lawful and ethical to do so and when this supports an appropriate purpose.

## 1.4 Scope

This policy covers all forms of information within the Trust, including (but not limited to):

- Service User information
- HR / Workforce information
- Organisational information
- Foundation Trust membership information
- Other personal confidential data
- Confidential Trust business & commercial information

This policy covers all aspects of handling information, including (but not limited to):

- Structured record systems – paper and electronic
- Transmission of information – fax, e-mail, post and telephone
- Movement of information – carried on digital media or in paper form

This policy covers all information systems used, purchased, developed and managed by or on behalf of the Trust and any individual directly employed by or associated with the Trust.

## 1.5 Openness

The Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. We will therefore seek to balance the public interest in providing a confidential service with our responsibilities under the Duty of Candour, the Freedom of Information Act and other relevant legislation and initiatives.

- Non-confidential information about the Trust and services will be available to the public through a variety of means, in line with the Trust's ethic of openness and the regulations outlined in the Freedom of Information Act.
- Patients will have access to information relating to their own health care, options for treatment and their rights – both as patients and as 'data subjects'. There will be clear procedures and arrangements for handling queries from patients and the public.
- Disclosure under Data Protection Act Subject Access Requests will be assessed for content which may cause risk of or actual harm and / or distress to the subject or any 3<sup>rd</sup> party. Such content may be withheld from disclosure.
- The Trust will have clear procedures and arrangements for liaison with the press and broadcasting media.
- Integrity of information will be developed, monitored and maintained to ensure that it is appropriate for the purposes intended.
- Availability of information for operational purposes will be maintained within set parameters relating to its importance via appropriate procedures and computer system & infrastructure resilience.
- The Trust regards all personal information relating to staff as confidential except where national policy on accountability and openness or other audit requirements dictate otherwise. Staff will however be identifiable by name in their professional capacity.
- The Trust will establish and maintain policies and procedures to ensure compliance with the Data Protection Act, the UK enactment of the EU General Data Protection Regulation, Human Rights Act, Computer Misuse Act, the common law duty of confidence and the Freedom of Information Act.
- Awareness and understanding of all staff with regard to responsibilities will be routinely assessed and appropriate training and awareness provided.
- Where appropriate, lawful and ethical, the Trust will share relevant information with partner organisations, subject to need.

## 1.6 Information Security

The Trust will establish and maintain policies and procedures for the effective and secure management of its information assets and resources.

- Audits will be undertaken or commissioned to assess information and IT security arrangements.
- The Trust Incident Reporting system will be used to report, monitor and investigate all breaches of confidentiality and information / cyber security. The IG Group will have sight of all IG-related reports and advise on further action if necessary.
- Near-miss reports will be evaluated to support future prevention.
- Any recurring themes in IG incidents will be followed up appropriately with trustwide communications.
- The Trust will monitor its systems and evaluate security arrangements against the evolving Information Governance agenda and any new directives or requirements received from NHS England, NHS Digital, the wider NHS and UK government sources.
- The Trust will monitor technical resources and horizon scan for new threats to information / cyber security.
- The IG Group, the IG team, and key ICT staff will contribute appropriate expertise to the information / cyber security aspects of the Information Governance Framework as required.

## 1.7 Information Quality Assurance

The Trust will establish and maintain policies and procedures for information quality assurance and the effective management of records.

- Audits will be undertaken or commissioned of the data quality and records management arrangements.
- All staff will be expected to take ownership of, and seek to improve, the quality of data within their services.
- Wherever possible, information quality will be assured at the point of collection.
- The Trust will promote data quality through policies & procedures, user manuals and appropriate training.
- The IG Group, Data Quality Group and the Informatics team will contribute appropriate expertise to the information quality assurance aspects of the Information Governance Framework as required.

## 1.8 Related Procedural Documents

The Trust has a comprehensive range of procedural documents supporting the Information Governance agenda; reference must be made to these alongside this policy. See Section 5 – Associated Documentation.

## 1.9 Legal / Ethical Context

The evolving Information Governance agenda is underpinned by several key legislative strands, NHS / DoH policy and other sectoral guidance; reference must be made to these alongside this policy. See Section 4 – References, Evidence Base.

## 1.10 Year-On-Year Improvement / Maintenance Plan and Assessment

An assessment of compliance with requirements within the NHS Digital Data Security & Protection Toolkit will be undertaken and continually monitored for progress against compliance. Reports and proposed action / development plans will be agreed and monitored by the IG Group.

## 1.11 Information Governance Group

Information Governance will be managed and championed across the Trust by the work of the Information Governance Group. The membership of this group will provide the Trust with an appropriate forum comprised of relevant expertise and representation.

- Caldicott Guardian (or Deputy)
- SIRO (or Deputy)
- Information & Knowledge Manager / Data Protection Officer / Freedom of Information Officer
- Information Governance Support Officer
- Chief Information Officer
- Head of Performance & Informatics
- Data Quality Manager
- Health Records Manager
- Human Resources representative
- ICT Network Support Manager
- IT Support Analyst
- Registration Authority Manager
- Clinical Directorate Information Leads (per Directorate)

The responsibilities of the Information Governance Group will include (but not be limited to):

- Recommending for approval, by the appropriate Trust Board or sub-committee, related policies and procedures.
- Recommending for approval to the Trust Board the annual submission of compliance with requirements in the NHS Digital Data Security & Protection Toolkit and related action plans.
- To co-ordinate and monitor Information Governance activity across the Trust.

- To evaluate information governance related incident reports (via DATIX), to assess the impact and action taken, to advise further action if required and to action trust-wide communications in the event of common incident themes.
- To receive reports and evaluate performance against the statutory requirements of the Freedom of Information Act and Subject Access Request performance under the Data Protection Act and the UK enactment of the EU General Data Protection Regulation.
- To track actions against the NHS Digital CareCERT cyber security threat broadcasts and monitor the state of preparedness against known cyber security threats.

For further information on the constitution, membership, remit and authority of the Information Governance Group, refer to the Group's Terms of Reference.

## 1.12 Duties and Responsibilities

The duties and responsibilities within the organisation are as follows. These duties also set out the Trust Information Governance Framework.

### **Chief Executive**

The Trust Chief Executive will be responsible for signing off appropriate declarations on behalf of the Trust and will be ultimately accountable for Information Governance issues.

### **Senior Information Risk Owner (SIRO)**

The Trust must have Board-level representation to act as the Senior Information Risk Owner (SIRO). This role is fulfilled by the Chief Financial Officer. The designated SIRO will act as the Board-level owner of information risks and as such will be the point of contact for Board-level input in this area. Progress against this Policy, particularly any difficulties and the resultant risks must be reported to the SIRO. The SIRO will be adequately trained via appropriate NHS Digital IG Training modules as a minimum, and will be supported by the Information and Knowledge Services department in this role.

### **Caldicott Guardian**

To be the Trust ultimate authority on patient confidentiality issues. Will advise on patient data confidentiality matters and provide this expertise to the IG Group by attendance at IG Group meetings. The Caldicott Guardian will be a Board-level member of the executive team and will be appropriately trained to ensure that knowledge and expertise remains current. The Caldicott Guardian will be supported by the Information and Knowledge Manager in the role of Deputy Caldicott Guardian.

## **Data Protection Officer / Freedom of Information Officer**

Will be the Trust first line of Information Governance expertise and as such an active participant in the IG Group. Will be the first point of call on data protection issues for staff or managers who need support in this area, referring to the Caldicott Guardian if required and specifically on patient confidentiality issues, and will support the Caldicott Guardian. Will oversee the Trust Freedom of Information Act and Data Protection Subject Access Request procedures and ensure that requests are processed in a timely and professional manner, with exemptions suitably and lawfully applied. The Data Protection Officer / Freedom of Information Officer will be appropriately trained and ensure that knowledge and expertise remains current. The Data Protection Officer / Freedom of Information Officer roles will be embodied in the post of Information and Knowledge Manager.

The Data Protection Officer will have statutory duties and responsibilities defined by the EU General Data Protection Regulation, which are as follows:-

GDPR - Article 39(1)(a)-(e) & (2)

- to inform and advise the most senior levels of management, Trust data controller, and their employees, of their obligations under the Regulation and other applicable laws and regulations
- to monitor compliance with the Regulation and other applicable laws and regulations and with the relevant policies of the Trust data controller, this includes assignment of responsibilities, awareness and training, and relevant audits. These reports will be provided to the most senior levels of management.
- to advise on the data protection impact assessment (DPIA) process and monitor its performance, if requested, and
- to liaise with the Information Commissioner's Office as required in the management of Information Governance breaches and general enquiries, seeking to protect the rights of patients, staff and the public
- in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.
- to be the advertised contact point for the public as regards the Regulation.

## **Information Governance Support Officer**

Will perform a key operational role in embedding and championing Information Governance in organisational culture. The IG Support Officer will facilitate both induction and formal IG training, assist in the drafting of IG related communications materials and support the activities of the IG Group as meeting facilitator. The post holder will operate and administer the Trust Freedom of Information procedures and assist on data protection and confidentiality issues. The Officer will be responsible for progress chasing the

NHS Digital Data Security & Protection Toolkit during each reporting year. The post holder will be appropriately trained and ensure that knowledge and expertise remains current.

### **Finance and Performance Committee**

Will support the IG team & IG Group in developing, enacting and ratifying IG oriented procedures and provide a mandate for work in this area. Where necessary they will evaluate Trust progress in the area of information security and provide budgetary support of this policy if required.

### **Information Governance Group**

Will support the IG team in developing and enacting this policy and will provide a forum to debate future developments in this area. They will interpret and advise on appropriate action in the light of any new guidance coming from NHS England, NHS Digital, NHS / DoH or Central Government. The group will be the appropriate reporting and investigatory body relating to IG incidents and will have oversight of Trust Data Security & Protection Toolkit progress and reporting.

### **Information Governance Team**

Will continue to monitor the evolving Information Governance agenda and make recommendations to revise this policy and any underlying procedures subject to need. The IG team will present any new directives in this area to the IG Group for consideration and action. The team will be responsible for providing any IG-related reporting to NHS England, NHS Digital, CQC, NHS Improvement and any other relevant body. The team will lead operationally on Data Security & Protection Toolkit performance.

### **Staff & Associated Non-Employed Personnel**

Will be personally responsible for making sure they adhere to the policy and all underlying procedures at all times. Every member of staff and all personnel working with / for the Trust but not employed by the Trust have a personal responsibility to observe best practice in the storage, handling, communicating and processing of all person-identifiable, sensitive and confidential information and remain vigilant to possible and actual breaches in information security and report them through the Trust incident reporting procedures. The Trust will provide compulsory IG training to all staff, with training a pre-requisite of Trust systems access. New staff will receive a basic IG awareness briefing at induction, and will maintain an awareness of IG communications via all media during their working lives within the Trust.

## 1.13 Training

The Information Governance team will take responsibility for raising the level of IG awareness and training throughout the Trust.

- All staff will attend, as part of their induction, an awareness session on Information Governance. This will be delivered via a presentation at the Trust's regular Corporate Induction events.
- The Trust compulsory Information Governance training package will be introduced to new starters via the Corporate Induction presentation during the induction event.
- Information Governance training is compulsory for all staff, in all staff groups / roles, on an annual basis.
- Information Governance training is compulsory pre-requisite for the following user groups:
  - a. Clinical systems users
  - b. Leeds Care Record users
  - c. E-Results users
  - d. Registration Authority SmartCard holders
- Failure to achieve and maintain the appropriate Information Governance training standard will result in the removal of access to Trust systems.
- The IG Team and IG Group will raise trustwide awareness of IG issues, common themes in incident reporting, training opportunities and progress etc. via appropriate communications methods.
- The IG Team will develop IG communications materials to inform and advise service users and staff on IG issues.

## 2 Appendices

None.

## PART B

### 3 IDENTIFICATION OF STAKEHOLDERS

The table below should be used as a summary. List those involved in development, consultation, approval and ratification processes.

Stakeholder	Level of involvement
Information Governance Group (comprising) <ul style="list-style-type: none"> <li>• Data Protection Officer</li> <li>• IG Support Officer</li> <li>• Chief Information Officer</li> <li>• ICT Service Desk Manager</li> <li>• ICT Support Analyst</li> <li>• Network Manager</li> </ul>	Consultation
Staffside representative	Consultation
Information Governance Group	Approval
Policy & Procedure Group	Ratification

### 4 REFERENCES, EVIDENCE BASE

- Data Protection Act
- UK enactment of the EU General Data Protection Regulation
- Human Rights Act
- Computer Misuse Act
- Freedom of Information Act
- Access to Health Records Act
- NHS Confidentiality Code of Practice
- Records Management Code of Practice for Health & Social Care
- Professional codes of conduct from the BMA, GMC and NMC and others including Allied Health professionals, Finance Professionals and NHS Managers

### 5 ASSOCIATED DOCUMENTATION (if relevant)

- IG-0002 – Health Records Policy
- IG-0003 – Confidentiality Code of Conduct
- IG-0004 – Forensic Readiness Policy
- IG-0005 – Freedom of Information Procedure
- IG-0006 – Data Quality Policy
- IG-0007 – Corporate Records Management Guidance
- IG-0008 – Data Protection Act - Subject Access Request Procedure
- IG-0009 – Safe Haven Guidance

- IT-0001 – Encryption Policy
  - IT-0002 – Internet Use Policy
  - IT-0003 – Email Use Policy
  - IT-0004 – Network Security Policy
  - IT-0005 – Portable Computing Device Policy
  - IT-0008 – Information Security Policy
  - IT-0009 – Supplier Support Access Agreement Procedure
  - IT-0010 – Mobile & Smartphone Communications Policy
- 
- IG Group Terms of Reference

## **6 STANDARDS/KEY PERFORMANCE INDICATORS (if relevant)**

Effectiveness of the policy will be monitored by the number and severity of IG incidents occurring within the Trust, and that the Trust remains free of adverse publicity and punitive sanctions imposed by the Information Commissioner or other regulatory body.

The NHS Digital Data Security & Protection Toolkit scoring (March 31<sup>st</sup>, annually) will also be viewed as an indicator of performance against this policy and the underlying procedural documents.

Regular reports of various aspects of IG performance will be supplied to the monthly IG Group meetings – see below:-

Topic	Monitoring/ Audit	Lead Manager	Data Source	Sample	Data Collection Method	Frequency Of Activity	Review Body
Data Security & Protection Toolkit results	Audit	Carl Starbuck	NHS Digital Toolkit website	Annual	Visit IG Toolkit website, internal monitoring SharePoint site	March 31 <sup>st</sup> (final)	IG Group
IG Incident Reporting	Monitoring	Carl Starbuck	Reports to IG Group	Monthly	Papers to Group	Monthly	IG Group
IG SIRI Reporting	Monitoring	Carl Starbuck	Reports to IG Group	Monthly	Papers to Group	Monthly	IG Group
Freedom of Information Act performance	Monitoring	Carl Starbuck	Reports to IG Group	Monthly	Papers to Group	Monthly	IG Group
Subject Access Request performance	Monitoring	Carl Starbuck	Reports to IG Group	Monthly	Papers to Group	Monthly	IG Group
IG Training compliance	Monitoring	Carl Starbuck	Reports to IG Group	Monthly	Papers to Group	Monthly	IG Group

## 7. EQUALITY IMPACT

The Trust has a duty under the Equality Act 2010 to have due regard to the need to eliminate unlawful discrimination, advance equality of opportunity and foster good relations between people from different groups. Consideration must be given to any potential impacts that the application of this policy/procedure might have on these requirements and on the nine protected groups identified by the Act (age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion and belief, gender and sexual orientation).

Declaration: The potential impacts on the application of this policy/procedure have been fully considered for all nine protected groups. Through this process I have not identified any potential negative impacts for any of the nine protected groups.

Print name: Carl Starbuck

Job title: Informaton & Knowledge Manager

Date: 17<sup>th</sup> April 2018

If any potential negative impacts are identified the Diversity Team must be contacted for advice and guidance: email; [diversity.lypft@nhs.net](mailto:diversity.lypft@nhs.net).

**CHECKLIST**

To be completed and attached to any draft version of a procedural document when submitted to the appropriate group/committee to support its consideration and approval/ratification of the procedural document.

This checklist is part of the working papers.

	<b>Title of document being newly created / reviewed:</b>	<b>Yes / No/</b>
<b>1.</b>	<b>Title</b>	
	Is the title clear and unambiguous?	✓
	Is the procedural document in the correct format and style?	✓
<b>2.</b>	<b>Development Process</b>	
	Is there evidence of reasonable attempts to ensure relevant expertise has been used?	✓
<b>3.</b>	<b>Content</b>	
	Is the Purpose of the document clear?	✓
<b>5.</b>	<b>Approval</b>	
	Does the document identify which committee/group will approve it?	✓
<b>6.</b>	<b>Equality Impact Assessment</b>	
	Has the declaration been completed?	✓
<b>7.</b>	<b>Review Date</b>	
	Is the review date identified?	✓
	Is the frequency of review identified and acceptable?	✓
<b>8.</b>	<b>Overall Responsibility for the Document</b>	
	Is it clear who will be responsible for co-ordinating the dissemination, implementation and review of the document?	✓

<b>Name of the Chair of the Committee / Group approving</b>			
If you are assured this document meets requirements and that it will provide an essential element in ensuring a safe and effective workforce, please sign and date below and forward to the chair of the committee/group where it will be ratified.			
Name	<i>Carl Starbuck</i>	Date	<i>26<sup>th</sup> April 2018</i>
<b>Name of the chair of the Group/Committee ratifying</b>			
If you are assured that the group or committee approving this procedural document have fulfilled its obligation please sign and date it and return to the procedural document author who will ensure the document is disseminated and uploaded onto Staffnet.			
Name		Date	