INFORMATION GOVERNANCE ASSURANCE FRAMEWORK STRATEGY

STRATEGY

Reference	IG/002
Approving Body	Trust Board
Date Approved	26.02.2018
Issue Date	26.02.2018
Version	2.1
Summary of Changes from Previous Version	Unified document for proposed new organisation
Supersedes	Information Governance Management Framework
Document Category	Information Governance
Consultation Undertaken	Information Governance Committee
Date of Completion of Equality Impact Assessment	June 2016
Date of Environmental Impact Assessment (if applicable)	Not applicable
Legal and/or Accreditation Implications	Adherence to Data Protection legislation
Target Audience	All staff
Review Date	Annual
Sponsor (Position)	Chief Executive
Author (Position & Name)	Information Governance Manager
Lead Division/ Directorate	Corporate
Lead Specialty/ Service/ Department	Information Governance
Position of Person able to provide Further Guidance/Information	Information Governance

Associated Documents/ Information	**Date Associated Documents/ Information was reviewed**
Not Applicable.	

Contents

This information can be made available in alternative formats, such as easy read or large print, and may be available in alternative languages, upon request. Please contact 01623 672531 or email mailto:sfh-tr.information.governance@nhs.net.

1.0 INTRODUCTION

1.1 The NHS Information Governance Assurance Framework (IGAF)

The Information Governance Framework for health and social care is formed by those elements of law and policy from which applicable information governance standards are derived, and the activities and roles which individually and collectively ensure that these standards are clearly defined and met.

While a key focus of information governance is the use of information about service users, it applies to information and information processing in its broadest sense and underpins both clinical and corporate governance. Accordingly it should be afforded appropriate priority.

1.2 Information Strategy

In 2012 the DoH published a 10-year framework for transforming information for health and care . It aims to harness information and new technologies to achieve higher quality care and improve outcomes for patients and service users. The strategy sets the following ambitions:

- Information used to drive integrated care across the entire health and social care sector, both within and between organisations
- Information regarded as a health and care service in its own right for us all – with appropriate support in using information available for those who need it, so that information benefits everyone and helps reduce inequalities
- A change in culture and mindset, in which our health and care professionals, organisations and systems recognise that information in our own care records is fundamentally about us – so that it becomes normal for us to access our own records easily
- Information recorded once, at our first contact with professional staff, and shared securely between those providing our care – supported by consistent use of information standards that enable data to flow (interoperability) between systems whilst keeping our confidential information safe and secure
- Our electronic care records progressively become the source for core information used to improve our care, improve services and to inform research, etc. – reducing bureaucratic data collections and enabling us to measure quality
- A culture of transparency, where access to high-quality, evidence-based information about services and the quality of care held by Government and health and care services is openly and easily available to us all
- An information-led culture where all health and care professionals – and local bodies whose policies influence our health, such as local councils – take responsibility for recording, sharing and using information to improve our care
- The widespread use of modern technology to make health and care services more convenient, accessible and efficient
- An information system built on innovative and integrated solutions and local decision-making, within a framework of national standards that ensure information can move freely, safely, and securely around the system.

1.3 NHS and the Information Commissioner

With changes to commissioning structures and increasingly diverse care providers, the NHS Chief Executive and the Information Commissioner have published a joint letter to ensure that we continue to give information governance the priority and attention it needs and signals the intention of the NHS and the Information Commissioner's Office to work together in supporting the NHS to deliver good information governance.

All NHS organisations (and others with access to NHS patient information) should:

a. be using the NHS Information Governance Toolkit https://www.igt.hscic.gov.uk/to assess and publish details of performance

b. ensure all staff undertakes appropriate information governance training annually as identified in the NHS Information Governance Toolkit .

c. have identified and trained a Board level individual to act as the Senior Information Risk Owner (SIRO) for the organisation

d. make staff aware continuously of the existing information governance policies and guidelines, the fact that they must be followed in practice, and that a breach of policy will be regarded as a disciplinary matter.

Also, the Information Commissioner has powers to conduct compulsory audits of NHS organisations and can fine data controllers up to £17million for serious data protection breaches.

1.4 Information Governance Toolkit

The annual information governance performance is measured via self-assessment of compliance against 45 requirements set out in the NHS Information Governance Toolkit and assured by Internal Audit. The requirements are spread across six categories:

i. Information Governance Management
ii. Information Security Assurance
iii. Confidentiality and Data Protection Assurance
iv. Clinical Information Assurance
v. Secondary Use Assurance
vi. Corporate Information Assurance.

The Trust is required to submit three IG performance reports:

31st Jul Baseline assessment of performance
31st Oct 2nd self-assessment or improvement report
31st Mar Final annual self-assessment report.

The final performance assessment is published on the NHS Digital website and is available to the public.

1.5 The IG Assurance Statement

As part of the IG Toolkit Assessment, the Trust is required to accept the IG Assurance Statement. This statement contains additional terms and conditions applicable to all organisations using NHS Digital services such as N3, and signifies an organisation's agreement to abide by those terms.

The IG Assurance Statement is binding on the Trust, and acceptance should be authorised by the senior executive and confirms the Trust's commitment to meeting and maintaining the required standards of information governance.

2.0 POLICY STATEMENT

2.0 Information Governance Objectives

2.1 The Strategy's objectives below set out to ensure the following primary aims of effective information governance are achieved:

i. Information will be organised, monitored and maintained in accordance with legal and regulatory frameworks and will be kept confidential where appropriate.
ii. The integrity of information will be assured, monitored and maintained, to ensure that it is of expected quality and reliable for use for the purposes that it is collected and used for.
iii. Information required for operational purposes will be kept secure and available to and accessed by those who need it.
iv. Relevant patient information will be shared with health and social care organisations to support direct patient care
v. All staff will have access to appropriate training and education to ensure they understand their responsibilities for managing information and follow the law.
vi. An information risk management strategy will be implemented to ensure ownership of and accountability for the Trust's information assets and the mitigation of associated risks.

2.2 The Trust will aim to achieve the specified performance level of compliance for all IG requirements and target year-on-year improvement.

All NHS organisations are expected to achieve a minimum level two performance (out of a maximum score of three) against all 45 requirements in the IG Toolkit. From 2015/16 twelve of these requirements have been mapped to the Caldicott 2 report recommendations and require attainment of 'level 3'.

A Toolkit Action Group (TAG), comprising owners of all Toolkit requirements and chaired by the IG Manager, has responsibility for:

- Reviewing changes to Toolkit requirements each year
- Developing actions plans to achieve target scores
- Monitoring progress and reporting to the IG Group.

The Trust's IG Toolkit performance will be monitored by the IG Group and our assessment will be reviewed by the SIRO prior to its submission to the NHS Digital.

2.3 The Trust will ensure that adequate governance arrangements are in place to support the IGAF agenda.

This will be achieved through compliance with the Information Governance Management Assurance standards.

The Information Governance Group will be responsible for steering the Trust's IG agenda. Appropriate organisational and management structures will be in place to support the Information Governance work programme.

2.4 IG Training for staff is mandated annually

Awareness and training needs to be provided to all Trust staff who utilise information in their day-to-day work to promote an information governance culture.

All staff, whether permanent, temporary or contracted, should be aware of their own individual responsibilities for the maintenance of confidentiality, data protection, information security management and information quality.

2.5 The Trust will establish a programme to measure and report IG performance

The Trust's IG performance will be measured through an annual:

- IG Toolkit self-assessment, which is reported regularly to the IG Group
- Internal audit of IG Toolkit evidence
- IG work plan
- IG self-assessment report from each IAO.

The IG Group will be responsible for challenging information governance performance and ensuring actions are taken to address shortfalls.

The SIRO will report on IG performance annually to the Trust Board.

2.6 The Trust will ensure patients and the public are effectively informed about how we use their information, and know how to access their information and exercise their information sharing preferences.

The Trust will develop and maintain a communications strategy to ensure that patients and the public are adequately informed about confidentiality and the way their information is used and shared, their rights as data subjects, in particular how they may access their personal data and how they may exercise those rights when consent is required to use their data for non-healthcare purposes. Effective procedures will be introduced to ensure that detailed questions raised by patients can be answered and their right of choice can be exercised and respected.

2.7 The Trust will ensure the confidentiality of personal information

The Trust will ensure that patient confidentiality is maintained in accordance with the DoH Confidentiality: NHS Code of Practice and legal requirements under the Data Protection Legislation, European Convention of Human Rights (Article 8) (Human Rights Act 1998) and common law.

The Trust will also ensure the protection of its staff's personal information in accordance with the Data Protection Legislation and Human Rights Act 1998.

2.8 The Trust will ensure the security of information
The Trust will protect personal data held in its information systems through compliance with the DoH Information Security Code of Practice and associated standard of ISO/IEC 27002:2013.
The Trust will ensure personal data is protected in accordance with DoH directives; by applying organisational, physical and electronic controls including encryption.

2.9 The Trust will provide assurance that all information risks are idThe Trust's information risk strategy will be embedded within established risk management arrangements.
Risks to the Trust's information assets will be managed in accordance with the risk management policy.

The Trust will include within its operational risk profile standard risk definitions for risks to the confidentiality, integrity and availability of information.
Corporate risks to digital continuity and compliance with statutory duties and regulations will also be recorded within the Trust's risk register.

The management of cyber security within the Trust will be based on the 10 Steps to Cyber Security issued by the National Cyber Security Centre (NCSC). The Trust will work with its Information Technology (IT) service provider, Nottinghamshire Health Informatics Service (NHIS) to develop and deliver a Cyber Security Strategy that is aligned to this framework.
The Trust will maintain clear lines of accountability for information risk management that lead directly to the Board through the appointment of a SIRO, IAOs and the development and maintenance of an Information Asset Register.

The SIRO and IAOs and IAAs will be accountable to the Accountable Officer for the management and mitigation of information risks and will provide assurance to that effect for the Annual Report and Statement of Internal Control.

Regular reports on the information risk profile and delivery of the Cyber Security Strategy will be reported to the SIRO.

Detailed responsibilities of the SIRO, IAOs and IAAs are at Appendix D. entified, managed and mitigated.

2.10 The Trust will ensure that clinical and corporate records, whether held in paper or electronic format, are managed in accordance with mandated and statutory requirements
The Trust will ensure that Health Records are managed in accordance with the Department of Health Records Management: NHS Code of Practice. This is set out in the Trust's Health Records Management Strategy.

The Trust will ensure compliance with the Freedom of Information Act 2000 and associated Lord Chancellor's Codes of Practice under sections 45 and 46. This is set out in the Trust's Corporate Records Management Strategy.

The Trust will ensure that its Data Protection notification is reviewed and updated annually and accurately reports all processing of personal data within the organisation.
The Trust, as the legal entity, will ensure that its personal data is controlled and managed in accordance with the terms of the Data Protection Legislation principles.

2.11 The Trust will ensure information governance is integrated into the Trust's Governance structure.
All Divisions (and Departments) should engage with and support the information governance programme of work and will ensure they are adequately represented on the Information Governance Group. Divisional governance arrangements should include IG to communicate, inform, action, measure and report the implementation and progress of the relevant standards within their areas of responsibility.

Managers are responsible for ensuring that the policy, supporting standards and guidelines are incorporated into work processes and there is on-going compliance.
Divisional IG performance will feature at least twice-yearly in Divisional performance meetings.

3.0 DEFINITIONS/ ABBREVIATIONS

Glossary

CQC	Care Quality Commission
DoH	Department of Health
HSCIC	Health and Social Care Information Centre
IAA	Information Asset Administrator
IAO	Information Asset Owner
ICO	Information Commissioner's Office
IG	Information Governance
IGAF	Information Governance Assurance Framework
NCRS	NHS Care Records Service
SIRI	Serious Incident Requiring Investigation
SIRO	Senior Information Risk Owner
TAG	Toolkit Action Group

4.0 ROLES AND RESPONSIBILITIES

4.1 Committees

Trust Board

The NHS Chief Executive has made it clear that ultimate responsibility for information governance in the NHS rests with the Trust Board of each organisation, who should note that:

- Information governance must be explicitly referenced within each organisation's statement of internal controls.
- A board-level SIRO is required in each organisation and an Information Asset Owner/Administrator should be designated for each separate database or other major information asset.
- Appropriate information governance training is mandatory for all users of personal data and for all those in key roles.
- The annual information governance assessment, via the Information Governance Toolkit, will continue with performance assessments submitted by 31st March each year, shared with the Care Quality Commission, Audit Commission, Monitor and NHS Digital. The results are made available to the public. NHS organisations must baseline their performance within the Toolkit by the end of July each year, and should update that assessment with improvements at the end of October to enable performance and actions to be tracked by monitoring bodies.
- Health and social care organisations are expected to achieve 'level 2' performance against all requirements identified in the Information Governance Toolkit. From 2015/16, in order to demonstrate compliance with the recommendations of the Caldicott 2 reports, 12 requirements and mandatory at level 3. Organisations must sign the Information Governance Statement of Compliance (IGSoC) to provide assurance that they are meeting key requirements and must have robust improvement plans to address any shortfalls against other requirements.

Details of Serious Incidents Requiring Investigation (SIRIs) involving actual or potential loss of personal data or breach of confidentiality must be reported to the Information Commissioner (via the IG Toolkit).

Senior Management Team

The Senior Management Team is responsible for Information Governance in accordance with their responsibility for the Trust's Risk Management Strategy.

The Senior Management Team will ensure the effectiveness and integration of the Information Governance arrangements.

While overall responsibility lies with the Trust Board, Divisional and Corporate Directors are responsible for ensuring that information governance is afforded the same priority as clinical and corporate governance and for implementing the information governance strategy and associated policies.

Information Governance Group
The Information Governance Group has responsibility for overseeing the implementation of this strategy, the Information Governance Policy and the annual IG improvement plan.
The Information Governance Group reports to the Senior Management Team.

Due to the wide scope of information governance, the Information Governance Committee also updates the Audit and Assurance Committee.

The Information Governance Group is required to report the result of self-assessment audits to the Trust Board for approval and in particular prior to its final submission to the Department of Health NHS and onwards.

The terms of reference for the Information Governance Group are at Appendix A.

4.2 Individual Officers

Chief Executive
The Chief Executive as the Accountable Officer for the Trust has overall accountability and responsibility for information governance in the Trust and is required to provide assurance through the Statement of Internal Control that all risks to the Trust, including those relating to information, are effectively managed and mitigated. Details of SIRIs involving data loss or confidentiality breach must also be reported in the annual report.

As the Senior Executive of the Trust the Chief Executive should authorise the IG Assurance Statement , which includes:

- The requirement that no patient identifiable data or other sensitive data be stored or processed offshore where the location is deemed non-compliant with the NHS Offshore Policy
- The right to audit by NHS Digital or nominated third parties
- Change Control Notification procedures and approvals processes
- The requirement for organisations to achieve, or be working towards, ISO27001
- The requirements for reporting security events and incidents.

Senior Information Risk Owner (SIRO)
The SIRO is responsible to the Chief Executive for information governance and takes ownership of the Trust's information risk policy, acts as advocate for information risk on the Board and provides written advice to the Accounting Officer on the content of the Statement of Internal Control in regard to information risk. The SIRO also reports annually to the Trust Board on information governance performance.

Caldicott Guardian

The Caldicott Guardian is the "conscience" of the organisation, providing a focal point for patient confidentiality and information sharing issues and advising on the options for lawful and ethical processing of information as required.

Information Asset Owners (IAOs)

Directors (or another member of the Divisional Management Team) are designated Information Asset Owners (IAOs) with responsibility for providing assurance to the SIRO that information is effectively managed within their Division/Department. This includes ensuring:

- Information risks within their Division/Department have been identified, recorded and controls are in place to mitigate those risks, for example,:
  - New or changed information systems do not pose unacceptable confidentiality and information security risks (see Privacy Impact Assessment at Appendix B)
  - Transfers of personal data are lawful and secure
  - Information assets are recorded in the Information Asset Register and regularly risk assessed
  - IG issues/incidents are reported and investigated in accordance with the Trust's procedures
  - Staff receive appropriate IG training for their role
  - Conducting periodic confidentiality audits
- Their Division/Department is represented on the Information Governance Group Appropriate Division/Department structures are in place to support the information governance agenda
- Information governance is reported to the Divisional governance forum or group as per Integrated Governance
- Reports on progress are submitted annually to the SIRO (see Appendix C).

Information Asset Administrators (IAAs)

IAOs are encouraged to appoint Information Asset Administrators (IAAs) to support them in the delivery of their information management responsibilities for the Division/Department. IAAs ensure that policies and procedures are followed, recognise actual or potential security incidents and take steps to mitigate those risks, consult their IAO on incident management, and ensure that information asset registers are accurate and up to date.

NB. Roles and responsibilities of the SIRO, IAOs and IAAs are set out at Appendix D.

Information Governance Manager

The Information Governance Manager is accountable to the SIRO and is responsible for ensuring the development and implementation of this strategy and for the delivery of the IGAF agenda.

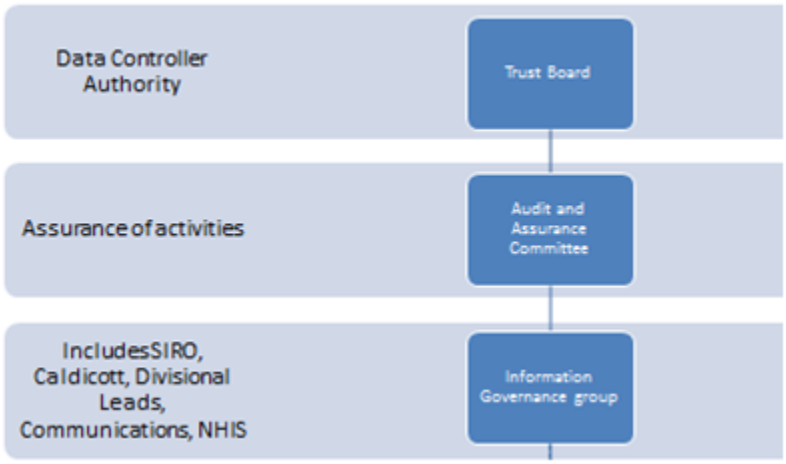
All Employees
All employees and anyone else working for SFH (e.g. agency staff, honorary contracts, management consultants etc.) who use and have access to Trust information must understand their personal responsibilities for information governance and comply with the law.
All staff must comply with Trust policies, protocols, procedures and guidance and attend relevant education and training events.

5.0 APPROVAL

This strategy is approved by Trust Board.

6.0 DOCUMENT REQUIREMENTS

Information Governance Resources
To support the IG Assurance Framework SFH has established an information governance structure with the primary objective to proactively promote good practice throughout the Trust. The structure is:



Management of IG Incidents
The IG Team monitors IG-related incidents logged in DATIX and will follow up all IG incidents to achieve a satisfactory outcome in liaison with investigating managers. More serious incidents are managed using the Trust's Incident Reporting Policy and Procedures. All IG incidents are reported to the IG Group, which will escalate any unsatisfactory outcomes to the Senior Management Team, and communicate pertinent IG issues/messages to staff using, for example, Trust Briefing and intranet notice board bulletins/icare2.

7.0 MONITORING COMPLIANCE AND EFFECTIVENESS

Minimum Requirement to be Monitored (WHAT – element of compliance or effectiveness within the document will be monitored)	Responsible Individual (WHO – is going to monitor this element)	Process for Monitoring e.g. Audit (HOW – will this element be monitored (method used))	Frequency of Monitoring (WHEN – will this element be monitored (frequency/ how often))	Responsible Individual or Committee/ Group for Review of Results (WHERE – Which individual/ committee or group will this be reported to, in what format (eg verbal, formal report etc) and by who)
Adherence to IG policies and procedures in nominated Division	360 Assurance	Audit	Annually	IG Group/IG Manager/Audit and Assurance Committee/IG Group
IG toolkit validation	360 Assurance	Audit	Annually	IG Group/IG Manager/Audit and Assurance Committee/IG Group

8.0 TRAINING AND IMPLEMENTATION

The Strategy will be made available via the Trust's Intranet and will be brought to the attention of all IAOs and IAAs.

The Information Governance Committee will ensure this strategy is reviewed at least every two years.

The Information Governance Group will provide assurance that it has been reviewed but will not submit the strategy for ratification unless changes and updates need to be made.

The Information Governance Group will review the Annual Plan each year in accordance with the programme for publication of the toolkit and baseline assessment (July/August) and issue that Annual Plan to the Audit and Assurance Committee for approval.

9.0 IMPACT ASSESSMENTS

Following the initial screening of this policy, a full impact assessment is not required at present as the policy does not create any environmental impact.

See Appendix E. SFH is committed to ensuring that none of its policies, procedures, services, projects or functions discriminate unlawfully. In order to ensure this commitment all policies, procedures, services, projects or functions will undergo an Equality Impact Assessment.

Reviews of Equality Impact Assessments will be conducted in line with the review of the policy, procedure, service, project or function.

10.0 EVIDENCE BASE (Relevant Legislation/ National Guidance) AND RELATED SFHFT DOCUMENTS

Evidence Base:

NHS Digitalhttp://systems.hscic.gov.uk/infogov
Confidentiality NHS Code of Practice
http://systems.hscic.gov.uk/infogov/codes
Information Security Management: NHS Code of Practice
http://systems.hscic.gov.uk/infogov/codes
NHS Care Record Guarantee
http://systems.hscic.gov.uk/rasmartcards/strategy/nhscrg
The Operating Framework for the NHS in England 2012/13 Department of Health
http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_131360
NHS Digital Information Governance publication and related links
http://systems.hscic.gov.uk/infogov/links

Related SFHFT Documents:

- Corporate Records Policy
- Data Protection, Confidentiality and Disclosures Policy
- Data Quality Policy
- Email Policy
- Freedom of Information Act Policy and Procedure
- Health Records Policy
- Information Governance Policy
- Information Security and Risk Policy
- Internet & Email Policy
- Retention and Destruction Policy

11.0 APPENDICES

APPENDIX 1 - EQUALITY IMPACT ASSESSMENT FORM (EQIA)

Name of service/policy/procedure being reviewed:			
New or existing service/policy/procedure:			
Date of Assessment:			
For the service/policy/procedure and its implementation answer the questions a – c below against each characteristic (if relevant consider breaking the policy or implementation down into areas)			
Protected Characteristic	**a) Using data and supporting information, what issues, needs or barriers could the protected characteristic groups' experience? For example, are there any known health inequality or access issues to consider?**	**b) What is already in place in the policy or its implementation to address any inequalities or barriers to access including under representation at clinics, screening?**	**c) Please state any barriers that still need to be addressed and any proposed actions to eliminate inequality**
The area of policy or its implementation being assessed:			
Race and Ethnicity	None	Not applicable	Not applicable
Gender	None	Not applicable	Not applicable
Age	None	Not applicable	Not applicable
Religion	None	Not applicable	Not applicable
Disability	None	Not applicable	Not applicable
Sexuality	None	Not applicable	Not applicable
Pregnancy and Maternity	None	Not applicable	Not applicable
Gender Reassignment	None	Not applicable	Not applicable
Marriage and Civil Partnership	None	Not applicable	Not applicable
Socio-Economic Factors (i.e. living in a poorer	None	Not applicable	Not applicable

neighbourhood / social deprivation)			

What consultation with protected characteristic groups including patient groups have you carried out?
None.

What data or information did you use in support of this EqIA?
None.

As far as you are aware are there any Human Rights issues be taken into account such as arising from surveys, questionnaires, comments, concerns, complaints or compliments?
None.

Level of impact

Low Level of Impact

Name of Responsible Person undertaking this assessment: Information Governance Manager

Signature:

Date: February 2018

APPENDIX 2 – ENVIRONMENTAL IMPACT ASSESSMENT

The purpose of an environmental impact assessment is to identify the environmental impact, assess the significance of the consequences and, if required, reduce and mitigate the effect by either, a) amend the policy b) implement mitigating actions.

Area of impact	Environmental Risk/Impacts to consider	Yes/No	Action Taken (where necessary)
Waste and materials	• Is the policy encouraging using more materials/supplies? • Is the policy likely to increase the waste produced? • Does the policy fail to utilise opportunities for introduction/replacement of materials that can be recycled?	No	
Soil/Land	• Is the policy likely to promote the use of substances dangerous to the land if released? (e.g. lubricants, liquid chemicals) • Does the policy fail to consider the need to provide adequate containment for these substances? (For example bunded containers, etc.)	No	
Water	• Is the policy likely to result in an increase of water usage? (estimate quantities) • Is the policy likely to result in water being polluted? (e.g. dangerous chemicals being introduced in the water) • Does the policy fail to include a mitigating procedure? (e.g. modify procedure to prevent water from being polluted; polluted water containment for adequate disposal)	No	
Air	• Is the policy likely to result in the introduction of procedures and equipment with resulting emissions to air? (For example use of a furnaces; combustion of fuels, emission or particles to the atmosphere, etc.) • Does the policy fail to include a procedure to mitigate the effects? • Does the policy fail to require compliance with the limits of emission imposed by the relevant regulations?	No	
Energy	• Does the policy result in an increase in energy consumption levels in the Trust? (estimate quantities)	No	
Nuisances	• Would the policy result in the creation of nuisances such as noise or odour (for staff, patients, visitors, neighbours and other relevant stakeholders)?	No	

APPENDIX 3: INFORMATION GOVERNANCE GROUP TERMS OF REFERENCE

Introduction
INFORMATION GOVERANCE GROUP (IG GROUP)
TERMS OF REFERENCE – Draft 8.4 2015

1. Remit

The purpose of this group is to share best practice and to advise on the development of a robust Information Governance Framework across the Trust.

2. Responsibilities

To provide a rolling programme of assurance, sharing best practice and to advise on the development of a robust Information Governance Framework across the Trust

To ensure that the Trust has effective policies and management arrangements covering all aspects of Information Governance in line with the Trust's overarching Information Governance Policy, which covers the four core aspects:

- Openness
- Legal Compliance
- Information Security
- Information Quality Assurance

To ensure that the Trust undertakes or commissions annual assessments and audits of its Information Governance policies and arrangements, namely completion of the Information Governance Toolkit in conjunction with NHS Digital.

To establish an annual Information Governance Work Plan and monitor progress against that plan.

To receive and consider reports on breaches of confidentiality and security. Where appropriate act as a 'Task and Finish' group to undertake or recommend actions to prevent similar incidents from reoccurring.

To report to the Audit and Assurance Committee and provide regular updates on progress against the annual Information Governance work plan.

To review and approve action plans for individual Information Governance initiatives.

To ensure annual completion of mandatory Information Governance training is completed across the Trust and that areas of non-compliance are followed up with the appropriate Division.

To identify areas of good Information Governance practice and disseminate across all appropriate areas of the Trust.

To engage with key stakeholders and take decisions on contentious Freedom of Information Act (FOIA) matters. The Group will also receive quarterly reports regarding the number of FOIA requests received and any trends identified.

To approve mitigating actions in relation to identified Information Governance risks that may occur as a result of NHS Digital project plans.

To provide a supporting function to the Caldicott Guardian and Senior Information Risk Owner (SIRO) and receive relevant escalated issues and updates from the Trust's Caldicott Group.

3. Membership

Senior Information Risk Owner (SIRO) (Chair)
Information Governance Manager
Caldicott Guardian
Head of Corporate Affairs and Company Secretary
Patient Services Manager
Workforce Information Manager
Head of Governance
Head of IT

In Attendance

Partnership Working Staff Side Lead
Divisional Lead or deputy for: Emergency Care, Medicine, Surgery, Women & Children, and Diagnostics and Outpatients
Head of Information
Head of Communication
Information Governance Coordinator
Head of Compliance and Systems
Training & Development Manager

The sub-group, or its Chairperson on its behalf, may co-opt or invite to meetings such other Trust officers as may be required.

4. Attendance
Members are expected to be active participants of the group and regular attendance is required with the expectation that all members (or their deputies as applicable) will attend 75% of the scheduled meetings.

If a member is unable to attend a meeting, where applicable, their nominated deputy must attend on their behalf and bring the members comments and/or their own comments to the meeting for discussion.

In the absence of a deputy, apologies/comments must be e mailed or sent by post to the secretary at the latest, the day prior to the meeting.

5. Meeting Frequency
The group will meet every month

6. Quorum
The quorum for this group is 4 members including either the SIRO or the Caldicott Guardian.

The Chairman of the group has the overriding and final decision in approving any documentation and or agreeing any other actions.

7. Reporting

The Chairman of the group will submit a report to the Risk Management Committee on a quarterly basis, but will escalate any urgent issues of concern to the relevant lead or committee as and when required.

8. Access to Group

Any member of staff can contact the Group for clarification of points associated with Information Governance practice or minutes of their meetings.
Agenda items should be brought to attention of the chairman or the Information Governance Manager and minutes will be circulated to Group members and any staff member who requests a copy.

APPENDIX 4 – INFORMATION GOVERNANCE GROUP MEMBERSHIP AND CONTACT LIST

ROLE	NAME (S)	DEPUTY
Senior Information Risk Owner (SIRO) (chair)	Paul Robinson	
Information Governance Manager	Jacquie Widdowson	
Caldicott Guardian	Andy Haynes	
Head of Corporate Services & Company Secretary	Shirley Clarke	
Patient Services Manager	Ann Gray	
Workforce Information Manager		
Divisional Lead or deputy for : Emergency Care, Medicine, Surgery, Women & Childrens and Diagnostics and Outpatients	Dale Travis (EC) Elaine Torr (D&O) Trevor Hammond (S) Haaris Mian(M) Simon Hallion (W&C)	
Head Of Governance	Denise Berry	
Head of IT		
Information Governance Coordinator	Joseff Eynon-Freeman Katie Towndrow	

APPENDIX 5: PRIVACY IMPACT ASSESSMENT TEMPLATE

PIA Template - Questionaire Final.do

APPENDIX 6: IG ANNUAL REPORT TO THE SIRO

IAO Template Report.doc

IAO Sign off Template (3).doc

APPENDIX 7: ROLES AND RESPONSIBILITIES OF SIRO, IAO, IAA

ROLES AND RESPONSIBILITIES OF

APPENDIX 8 - CERTIFICATION OF EMPLOYEE AWARENESS

Document Title	INFORMATION GOVERNANCE ASSURANCE FRAMEWORK STRATEGY
Version (number)	2.1
Version (date)	26.02.2018

I hereby certify that I have:

- Identified (by reference to the document control sheet of the above policy/ procedure) the staff groups within my area of responsibility to whom this policy / procedure applies.
- Made arrangements to ensure that such members of staff have the opportunity to be aware of the existence of this document and have the means to access, read and understand it.

Signature	
Print name	
Date	
Division/ Department	

The manager completing this certification should retain it for audit and/or other purposes for a period of six years (even if subsequent versions of the document are implemented). The suggested level of certification is;

- Clinical Divisions – Divisional General Manager or nominated deputy
- Corporate Departments - Deputy Director or equivalent.

The manager may, at their discretion, also require that subordinate levels of their / department utilise this form in a similar way, but this would always be an **additional** (not replacement) action.