C:\Documents and Settings\helen.sanderson\Local Settings\Temporary Internet Files\Content.Outlook\6UXB7KOT\NLlogo.png

**Information Governance Framework and Strategy**

|  |  |
| --- | --- |
| **Authorship:** | Information Governance |
| **Committee Approved:** | IGSG & SIRO following minor changes. |
| **Approved date:** | 21/01/2022 |
| **Review Date:** | December 2023 |
| **Equality Impact Assessment Quality Impact Assessment**  **Sustainability Impact Assessment**  **Data Protection Impact Assessment**  **Target Audience:** | **Completed Completed Completed**  **Not applicable**  **All Staff** |
| **Policy Reference No:** | N/A |
| **Version Number:** | 4.0 |

**The on-line version is the only version that is maintained. Any printed copies should, therefore, be viewed as ‘uncontrolled’ and as such may not necessarily contain the latest updates and amendments.**

## POLICY AMENDMENTS

Amendments to the Policy will be issued from time to time. A new amendment history will be issued with each change.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **New**  **Version Number** | **Issued by** | **Nature of Amendment** | **Approved by & Date** | **Date on Intranet** |
| 0.1 | Barry Jackson | First draft for comments | NR |  |
| 1.0 | Barry Jackson | Approved version | November 2015 |  |
| 1.1 | Helen Sanderson | Addition of DH Guidance re applications from those who cannot put a request in writing.  Addition of reference Materials |  |  |
| 2 | Kath Allen | Addition of Impact Analysis sections (2) Minor amendments to reflect change from CSU to EMBED  More details of accountability processes and organisational structure (16) and inclusion of IGSG TOR Training & Guidance removed reference to current training tool (13) | Quality Working Group |  |
| 2.1 | Mark Culling | Amendments to reflect the Data Protection Act 1998 (expected to be superseded by a Data Protection Act 2017 incorporating the requirements of the General Data  Protection Regulation). |  |  |
| 2.2 | Mark Culling | Annual review – updated references to new DSP Toolkit and new DPA/GDPR  legislation |  |  |
| 3.0 | Kath Allen | Annual review – bring up to date with new  DSPT requirements |  |  |
| 4.0 | Hayley Gillingwater | Updates to:  Introduction  Job Titles  Caldicott Principles  DSPT  Data Protection Officer  Information Security  Bribery Act  Removal of TNA  Terms of Reference | IGSG & SIRO – 21/01/22 |  |

## CONTENTS

|  |  |  |
| --- | --- | --- |
| **No** | **Subject** | **Page** |
| 1 | Introduction & Purpose | 4 |
| 2 | Information Governance Strategy | 4 |
| 3 | National Context | 4 |
| 4 | Aim | 4 |
| 5 | Data Security & Protection Toolkit | 5 |
| 6 | Roles & Responsibilities | 5 |
|  | 6.1 Information Governance Provider | 5 |
|  | 6.2 Governing Body | 5 |
|  | 6.3 IA&G | 5 |
|  | 6.4 IG Steering Group | 6 |
|  | 6.5 Caldicott Guardian | 6 |
|  | 6.6 SIRO | 6 |
|  | 6.7 Data Protection Officer | 7 |
|  | 6.8 Information Governance Lead | 7 |
|  | 6.9 Information Asset Owners & Administrators | 8 |
|  | 6.10 Managers | 8 |
|  | 6.11 All staff | 8 |
|  | 6.12 Third Party Contractors | 9 |
| 7 | Governance Arrangements | 9 |
| 8 | Key Principles and Procedures | 10 |
|  | 8.1. Openness and Transparency | 10 |
|  | 8.2 Legal Compliance | 10 |
| 9 | Information Security | 11 |
|  | 9.1 Quality Assurance and Records Management | 12 |
| 10 | Impact Analyses | 12 |
|  | 10.1 Equality | 12 |
|  | 10.2 Sustainability | 12 |
|  | 10.3 Quality | 12 |
|  | 10.4 Bribery Act 2010 | 12 |
| 11 | Data Protection Act | 13 |
| 12 | Caldicott Principles & Requirements | 14 |
| 13 | Handling Confidential Information | 14 |
| 14 | Risk Management | 15 |
| 15 | Training & Guidance | 15 |
| 16 | Awareness & Advice | 17 |
| 17 | Incident Management | 17 |
|  | 17.1 Incident Reporting | 17 |
|  | 17.2 Investigation | 18 |
| 18 | Organisational Structure for IG Reporting & Assurance | 18 |
| 19 | Policies & Procedures | 19 |
| 20 | Reference Material | 19 |
|  | **Appendices** |  |
| Annex A | NLCCG IG Strategy | 20 |
| Annex B | Data Protection Act Principles | 21 |
| Annex C | Caldicott Principles | 22 |
| Annex D | Everyone Counts; Planning for Patients | 23 |
| Annex E | Information Governance Steering Group TOR Jan 2021 | 24 |
| Annex F | Data Protection by design and default audit | 27 |
| Annex G | Triple Impact Assessment | 29 |

1. **Introduction and Purpose**

The purpose of this framework is to describe the management arrangements that will deliver Information Governance (IG) assurance within North Lincolnshire Clinical Commissioning Group (afterwards referred to as NLCCG). Information Governance is a framework that enables the organisation to establish good practice around the handling of information, promote a culture of awareness and improvement and comply with legislation and other mandatory standards.

Information Governance is about setting a high standard for the handling of information and giving organisations the tools to achieve that standard. The ultimate aim is to demonstrate that an organisation can be trusted to maintain the confidentiality and security of personal information, by helping individuals to practice good information governance and to be consistent in the way they handle personal and corporate information.

## Information Governance Strategy

The development of a fixed IG Framework will support an IG Strategy that will develop over time with the current version published at Annex A.

## National Context

The NHS Information Governance Assurance Programme (IGAP) was established in February 2008 in response to the Cabinet Office Data Handling review. The Prime Minister commissioned the review following the high-profile data losses in 2007.

IGAP developed a number of principles to support and strengthen the existing Information Governance agenda.

The principles are:

* + All NHS organisations should be part of the same Information Governance Assurance Framework (IGAF)
  + Information Governance should be as much as possible integrated into the broader governance of an organisation, and regarded as being as important as financial and clinical governance in organisational culture
  + The Framework will provide assurance to the several audiences interested in the safe custody and use of sensitive personal information in healthcare. This involves greater transparency in organisational business processes around Information Governance
  + IGAF to be built on the strong foundations of the existing Information Governance agenda and is the mechanism by which:
    - IG policies and standards are set
    - Regulators can check an organisation’s compliance
    - An organisation can be performance managed

## Aim

The purpose of this local framework is to set out an overall strategy and promote a culture of good practice around the processing of information and use of information systems. That is, to ensure that information is handled to ethical and quality standards in a secure and confidential manner. The organisation requires all employees to comply with the Policies, Procedures and Guidelines which are in place to implement this framework with the aim of ensuring that NLCCG maintains high standards of IG.

NLCCG will establish, implement and maintain procedures linked to this policy to ensure compliance with the requirements of the UK General Data Protection Regulation (GDPR) / Data Protection Act 2018. Records Management Guidance, Information Security Guidance and other related

legislation and guidance, contractual responsibilities and to support the assurance standards of the Data Security and Protection Toolkit. These standards are:

* + Information Governance Management
  + Confidentiality and Data Protection Assurance
  + Information Security Assurance
  + Clinical Information Assurance

This policy supports the CCG in its role as a Commissioner of Health Services and will assist in the safe sharing of information with its partner and agencies.

## Data Security and Protection Toolkit (DSPT)

The Data Security and Protection Toolkit (DSPT) is an online tool that enables organisations to measure their performance against the information governance requirements and compliance with the toolkit provides assurance that organisations have established good practice around the handling of information, are actively promoting a culture of awareness and improvement to comply with legislation and other mandatory standards.

Completion of the DSPT is mandatory for all organisations connected to N3 the proprietary NHS computer network, for organisations using NHS Mail and providing NHS services. All organisations are required to show compliance with assertions and (mandatory) evidence items. Annual plans will be developed year on year from the DSPT to achieve a satisfactory compliance with all assertions and (mandatory) evidence. As the DSP Toolkit is a publicly available assessment, the compliance of partner organisations in completing a DSP Toolkit will be used to assess their suitability to share information and to conduct business with.

## Roles and Responsibilities

* 1. **Information Governance Delivery Manager**
  2. **The Information Governance Delivery Manager will be responsible for ensuring appropriate policies and procedures are in place.**

## Governing Body

The Governing Body is accountable for ensuring that the necessary support and resources are available for effective implementation of this policy. It has the responsibility for the Information Governance Agenda supported by identified senior roles i.e. Caldicott Guardian, SIRO, DPO and IG Lead.

## The Integrated Audit & Governance Committee (IA&G)

The IA&G support and drive the broader information governance agenda and provide the Governing Body with the assurance that effective information governance best practice mechanisms are in place within the organisation.

The Information Governance agenda will be led by the SIRO supported by the IG Delivery Manager and will report through regular IG Meetings to the IA&G Committee.

The IG Work Programme, and new or significantly amended strategies and policies are escalated for consideration and approval to the IA&G Committee and the Governing Body.

## IG Steering Group

The Information Governance Steering Group (IGSG) is a standing group accountable to the IA&G Committee. The Group’s purpose is to support and embed the broader information governance agenda within the organisation and provide the Governing Body with assurance that effective information governance is in place within the organisation. The Group is responsible for the following arears of work

* + - Confidentiality & Consent
    - Data protection
    - Data Quality
    - Information Management
    - Information Disclosure and sharing
    - Information security
    - Records management
    - Registration Authority
    - Access Control
    - IG Incident Reporting
    - Freedom of Information
    - Data Privacy Impact assessments
    - Subject access requests

## Caldicott Guardian

The Caldicott Guardian for NLCCG is the Director of Nursing and Quality.

The Caldicott Guardian is a senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing. The Guardian plays a key role in ensuring that NHS and partner organisations satisfy the highest practical standards for handling patient identifiable information.

Acting as the 'conscience' of an organisation, the Guardian actively supports work to enable information sharing where it is appropriate to share, and advises on options for lawful and ethical processing of information. The Caldicott Guardian also has a strategic role, which involves representing and championing Information Governance requirements and issues at Board or management team level and, where appropriate, at a range of levels within the organisation's overall governance framework.

## Senior Information Risk Owner (SIRO)

The SIRO for NLCCG is the Chief Finance Officer.

The Senior Information Risk Owner (SIRO) is an Executive Director or Senior Management Board Member who will take overall ownership of the Organisation’s Information Risk Policy, act as champion for information risk

on the Board and provide written advice to the Accounting Officer on the content of the Organisation’s Annual Governance Statement in regard to information risk.

The SIRO must understand how the strategic business goals of the Organisation and how other organisations’ business goals may be impacted by information risks, and how those risks may be managed. The SIRO implements and leads the Information Governance (IG) risk assessment and management processes within the Organisation and advises the Board on the effectiveness of information risk management across the Organisation.

## Data Protection Officer

Under GDPR public authorities or organisations who carry out large scale processing of sensitive data must appoint a Data Protection Officer. (The DPO for NLCCG is provided by North Lincolnshire Council. The Data Protection Officer works with the IG Lead and the IG Delivery Manager to ensure systems and projects are safely developed and implemented. The role of Data Protection Officer is to facilitate the CCG’s compliance with GDPR and will:

* + - Monitor CCG compliance with the GDPR
    - Provide advice and assistance with regards to the completion of Privacy Impact Assessments
    - Act as a contact point for the Information Commissioners Office (ICO), members of the public and CCG staff on matters relating to GDPR and the protection of personal information
    - Assist in implementing essential elements of the GDPR such as the principles of data processing, data subjects’ rights, privacy impact assessments, records of processing activities, security of processing and notification and communication of data breaches

## Information Governance Lead

The Information Governance Lead for NLCCG is the Head of Governance.

The IG Lead works with the IG Provider to ensure systems are developed and implemented. The IG Lead is responsible for the co-ordination of the implementation within the CCG. The IG lead is accountable for ensuring effective management, accountability, compliance and assurance for all aspects of IG within the CCG. This role includes but is not limited to:-

* + - developing and maintaining the currency of comprehensive and appropriate documentation that demonstrates commitment to and ownership of IG responsibilities, e.g. an overarching high level strategy document supported by corporate and/or directorate policies and procedures;
    - ensuring that there is top level awareness and support for IG resourcing and implementation of improvements;
    - providing direction in formulating, establishing and promoting IG policies;
    - establishing working groups, if necessary, to co-ordinate the activities of staff given IG responsibilities and progress initiatives;
    - ensuring annual assessments and audits of IG policies and arrangements are carried out, documented and reported;
    - ensuring that the approach to information handling is communicated to all staff and made available to the public;
    - ensuring that appropriate training is made available to staff and completed as necessary to support their duties and for NHS organisations;
    - liaising with other committees, working groups and programme boards in order to promote and integrate IG standards;
    - monitoring information handling activities to ensure compliance with law and guidance; and
    - providing a focal point for the resolution and/or discussion of IG issues.

## Information Asset Owners and Administrators

Information Asset Owners (IAO) are senior individuals involved in the running of their respective business functions and are directly accountable to the SIRO. IAOs must provide assurance that information risk is being managed effectively in respect of the information assets they are responsible for and that any new changes introduced to their business processes and systems undergo a data protection impact assessment.

An Information Asset Administrator (IAA) will have delegated responsibility for the operational use of an Asset.

## Managers

Managers are responsible for ensuring that their staff, both permanent and temporary, are aware of:

* + - all information security policies and guidance and their responsibility to comply with them;
    - their personal responsibilities for information security;
    - where to access advice on matters relating to security and confidentiality; and
    - the security of their physical environments where information is processed or stored.

## All staff

Information Governance compliance is an obligation for all staff. Staff should note that they are expected to participate in induction training, annual refresher training and awareness raising sessions carried out to inform/update staff on information governance issues. Any breach of confidentiality, inappropriate use of health, business or staff records or abuse of computer systems is a disciplinary offence, which could result in dismissal or termination of employment contract and must be reported to the SIRO and (in the case of health or social care records), the Caldicott Guardian.

All employees are personally responsible for compliance with the law in relation to the Data Protection Act, the General Data Protection Regulation and the Common Law of Confidentiality.

Staff are responsible for reporting any possible or potential issues whereby a breach of security may occur.

## Third Party Contractors

Contracts with third parties providing services to NLCCG must include appropriate, detailed and explicit requirements regarding confidentiality and information governance to ensure that Contractors are aware of their IG obligations. Ideally the NHS Standard Contract should always be used where possible as this contains all necessary Information Governance clauses.

## Support services

All support services that process information on behalf of the CCG will be required to:

* + - Ensure a suitable contract/SLA and or as a minimum, a confidentiality agreement is in place to form a Controller to Processor relationship where Personal or Personal Sensitive data is managed on behalf of the CCG.
    - Ensure that services commissioned meet the requirements of the current Data Protection Act and GDPR when providing services including, but not limited to, fair processing and maintaining a Data Protection notification with the Information Commissioners Office.
    - Complete the annual Data Security and Protection Toolkit (if applicable), and at the request of the CCG, undertakes a compliance check/audit in order to provide assurance that they have met expected requirements.
    - Ensure that any new processing is within the remit of the contract or seek written confirmation if there is any ambiguity.
    - Report any known incidents or risks in relation to the use or management of information owned by the CCG.
    - Set out expectations regarding providing information in relation to requests for information made under the Freedom of Information Act.
    - Ensure inclusions regarding Exit Plans are addressed following transfer services or decommission of service e.g. passing on data/deletion/retention of data at the end of the contract.

## Governance Arrangements

The following arrangements have been agreed:

* + The CCG Governing Body will receive periodic assurance that management and accountability arrangements are adequate and are informed in a timely manner of future changes in the IG agenda by IG updates.
  + The CCG will obtain Information Governance Support via a shared service hosted by East Riding CCG governed by a Memorandum of Understanding.
  + Responsibility and accountability for Information Governance will be cascaded through the organization via staff contracts, contracts with third parties, Information Asset Owner arrangements and Heads of Service.

## Key Principals and Procedures

* 1. **Openness and Transparency**
     + The CCG recognizes the need for an appropriate balance between openness and confidentiality in the management and use of information.
     + Information will be defined and where appropriate kept confidential underpinning the principals of Caldicott legislation and guidance.
     + Information about the organization will be available to the public in line with the Freedom of Information Act, Environmental Information Regulations and Protection of Freedoms Act unless an exemption applies. The CCG will establish and maintain a Publication Scheme in line with the legislation and guidance from the Information Commissioner.
     + There will be clear procedures and arrangements for handling queries from patients, staff and other agencies and the public concerning personal and organizational information.
     + Integrity of information will be developed, monitored and maintained to ensure it is appropriate for the purposes intended.
     + Legislation, national and local guidelines will be followed
     + The CCG will undertake annual assessments and audits (through the Data Security and Protection Toolkit) of its policies, procedures and arrangements for openness.
     + Patients will have ready access to information relating to their own health care under Data Protection legislation using the CCG’s Access to Records policy.
     + The CCG will have clear procedures and arrangements for liaison with the press and broadcasting media.

## Legal Compliance

* + - The CCG regards all identifiable personal information relating to patients as confidential. Compliance with legal and regulatory requirements will be achieved, monitored and maintained.
    - The CCG will undertake or commission annual assessments and audits of its compliance with legal requirements as part of the Annual Assessment against the Data Protection and Security Toolkit Assertions and in line with changes and developments in legislation and guidance.
    - The CCG regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise as set out in the principals of the Human Rights Act and in the public interest.
    - The CCG will establish and maintain policies to ensure compliance with the current Data Protection legislation, Freedom of Information Act, Human Rights Act and the common law of confidentiality and associated guidance.
    - The CCG will work with partner NHS bodies and other agencies to establish Information Sharing Protocols to inform the controlled and appropriate sharing of patient information with other agencies, taking into account legislation.
    - Information Governance training will be mandatory for all staff. This will include awareness and understanding of Caldicott Principles and confidentiality, information security and data protection. Information Governance will be included in induction training for all new staff with completion of refresher training on an annual basis thereafter. The necessity and frequency of any further training will be personal development based.

The CCG will work in collaboration with the Local Counter Fraud Specialists and other related agencies to support their work in detecting and investigating fraudulent activity across the NHS.

## Information Security

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

* + The CCG will establish and maintain policies for the effective and secure management of its information assets and resources.
  + The CCG will undertake or commission annual assessments and audits of its information and IT security arrangements as part of the Annual Assessment against the Data Security and Protection Assertions and in line with changes and development in legislation and guidance.
  + The CCG will promote effective confidentiality and information security practice to its staff through policies, procedures and training.
  + The CCG will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.
  + The CCG will appoint a Senior Information Risk Owner and assign responsibility to Information Asset Owners to manage information risk.
  + The CCG will use pseudonymistaion and anonymization of personal data where appropriate to further restrict access to confidential information.
  + All new projects, processes and systems (including software and

hardware) which are introduced must meet confidentiality and data protection requirements. To enable the organization to address the privacy concerns a Data Protection Impact Assessment (DPIA) must be used. Under GDPR Data Protection Impact Assessments are mandated for high risk processing.

## Quality Assurance and Records Management

* + - The CCG will establish and maintain policies and procedures for information quality assurance and the effective management of records.
    - The CCG will undertake or commission annual assessments and audits of its information quality and records management arrangements.
    - Managers are expected to take ownership of, and seek to improve of, the quality of information within their services.
    - Wherever possible, information quality should be assured through policies, procedures, user manual and training.
    - Data standards will be set through clear and consistent definition of data items, in accordance with national standards.
    - The CCG will establish a Records Management policy covering all aspects of records management and consistent with the Records Management Code of Practice for Health and Social Care 2016.

## Impact Analyses

* 1. **Equality**

In developing this framework, an equality impact assessment has been completed. A full equalities impact assessment was deemed not to be required. This is because the policy is formatted in a way that is easy to read and can be made available on request in other formats and in other languages from the author of this framework. Arrangements can be made for members of staff with disabilities who wish to access information in a different format.

As a result of performing the analysis, the framework does not appear to have any adverse effects on people who share Protected Characteristics and no further actions are recommended at this stage; details are available alongside this framework on the CCG’s website.

## Sustainability

A sustainability Impact Assessment has been completed and details are available alongside this Framework on the CCG’s website. No impact on sustainability has been identified.

## Quality

A Quality Assessment has been completed

## Bribery Act 2010

The Bribery Act is particularly relevant to this policy.  The CCG has a responsibility to ensure that all staff are made aware of their duties and responsibilities arising from the Bribery Act 2010.  Under the Bribery Act 2010 there are four criminal offences:

•           Bribing or offering to bribe another person (Section 1)

•           Requesting, agreeing to receive or accepting a bribe (Section 2);

•           Bribing, or offering to bribe, a foreign public official (Section 6);

•           Failing to prevent bribery (Section 7).

These offences can be committed directly or by and through a third person and, in many cases, it does not matter whether the person knows or believes that the performance of the function or activity is improper.

It should be noted that there need not be any actual giving and receiving for financial or other advantage to be gained, to commit an offence.

All individuals should be aware that in committing an act of bribery they may be subject to a penalty of up to 10 years imprisonment, an unlimited fine, or both.  They may also expose the organisation to a conviction punishable with an unlimited fine because the organisation may be liable where a person associated with it commits an act of bribery.

Individuals should also be aware that a breach of this Act renders them liable to disciplinary action by the CCG, whether or not the breach leads to prosecution.  Where a material breach is found to have occurred, the likely sanction will be loss of employment and pension rights.

It is the duty of every member of staff to speak up about any genuine concerns in relation to criminal activity, breach of a legal obligation, miscarriage of justice, danger to health and safety or the environment and the suspected cover up of any of these in the workplace.  To raise any suspicions of bribery and/or corruption please contact the Chief Finance Officer.  Staff may also contact the Local Counter Fraud Specialist (LCFS) at – Audit Yorkshire, 01482 866800 email:  [nikki.cooper1@nhs.net](mailto:nikki.cooper1@nhs.net)  or mobile 07872 988939 or Head of Anti-Crime Services on 07717 356707 / email [steven.moss@nhs.net](mailto:steven.moss@nhs.net).

The  LCFS or Chief Finance Officer should be the contact for any suspicions of fraud. The LCFS will inform the Chief Finance Officer if the suspicion seems well founded and will conduct a thorough investigation.  Concerns may also be discussed with the Chief Finance Officer or the Audit & Integrated Governance Committee Chair.

If staff prefer, they may call the NHS Fraud & Corruption Reporting Line on 0800 028 40 60 between 8am-6pm Monday-Friday or report online at [www.reportnhsfraud.nhs.uk](http://www.reportnhsfraud.nhs.uk).  This would be the suggested contact if there is a concern that the LCFS or the Chief Finance Officer themselves may be implicated in suspected fraud, bribery or corruption.

.

## Data Protection Act (DPA)

The current Data Protection Act, incorporating the requirements of the General Data Protection Regulation (GDPR), are the most fundamental pieces of legislation that underpins Information Governance. NLCCG are registered with the Information Commissioners Office and will fully comply with all legal requirements of the Act. A process has been adopted to promote Data Protection by Design (please see Annex

F) and ensure that a review of all of new systems is carried out and where requirements such as the need for Data Protection Impact Assessments (DPIA) are highlighted, these will be completed.

The GDPR Principles relating to the processing of personal data are detailed at Annex B.

## Caldicott Principles and Requirements

The original Caldicott Report on the Review of Patient-Identifiable Information 1997 and the subsequent Report of the Caldicott2 Review - Information: To share or not to share? The Information Governance Review 2013. These two reports have identified specific principles that are considered essential practice for the appropriate sharing and security of Patient Information.

Government Response to the Report of the Caldicott 2 Report acknowledges the findings of this and promotes that everyone should understand how to protect and, where appropriate, share information about the people they care for, either directly or indirectly. The Caldicott Principles are detailed at Annex C.

This is further supported by the Everyone Counts: Planning for Patients 2014/15 to 2019/20 by detailing practical applications for information sharing, these are detailed at Annex D.

## Handling Confidential Information

When handling confidential information and especially where an individual can be identified from the information to be processed, the CCG must ensure that it has determined and documented a legal basis for processing that information.

In addition it must ensure that arrangements are in place to ensure:

* + Ensuring data subjects are appropriately informed of all uses of their information
  + The security of that information at all points of its lifecycle.
  + Recognising and recording objections to the handling of confidential information and where circumstances under which an objection cannot be upheld.
  + Ensuring that where objections are received where the proposed uses are not required by law the CCG should ensure they act in accordance with that objection.
  + Implement procedures for recognising and responding to individuals requests for access to their personal information.
  + Ensure appropriate information sharing arrangements are in place for the purposes of direct care.
  + Ensure appropriate data processing agreements are in place to collect or obtain information for management purposes.
  + Ensure staff are appropriately trained to handle confidential information
  + Ensure staff are aware of and follow data breach reporting processes

NHS Digital has issued two guidance documents in respect of appropriate information handling and confidentiality of that information:

1. **Code of practice on confidential information**: This code of practice describes good practice for organisations handling confidential information concerning, or connected with, the provision of health services or adult social care.
2. **A guide to confidentiality in health and social care**: A guide for those involved in the direct care of a patient on the appropriate handling of confidential information.

## Risk Management

The ability to apply good risk management principles to IG is fundamental and all organisations will apply them through organisational policies. The IG Team will be responsible for completion of the risk assessments for any IG related issue, and have a specific remit to risk assess new technologies and recommend controls where necessary.

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

## Training and Guidance

In accordance with the requirement to achieve compliance with the Data Security and Protection Toolkit all staff must complete an induction session, which will include Information Governance, when they first start employment. In subsequent years,

Data Security Awareness training is mandatory for all staff

and will include awareness and understanding of Caldicott principles and confidentiality, information security and data protection. E-learning products are provided for the training via the eLearning for Health website and ESR.

There will be specific modules available for Caldicott, SIRO and IG staff themselves. Appropriate staff must complete the modules relevant to their roles.

Please see the Training Needs Analysis to find out what training will be required for your role.

Staff awareness of IG will also be assessed by questions in the Annual Staff Survey in order to provide assurance that the training is sufficient.

O

s

## Awareness and Advice

The IG Delivery Manager will provide advice on any IG related issue. They will work with the NLCCG IG Lead to produce newsletters and staff e-mails to provide information and updates on IG issues.

## Incident Management

* 1. **Incident Reporting**

Information Governance and IT related incidents, including cyber security incidents (including but not limited to, physical destruction or damage to the organisation’s computer systems, loss of systems availability and the theft, disclosure or modification of information due to intentional or accidental unauthorised actions) must be reported and managed through the CCG’s Incident Management and Reporting Policy. Under GDPR, where a data breach is likely to result in a risk to the rights and freedoms of the individual, incidents must be reported to the Information Commissioners Office within 72 hours.

An information governance incident of sufficient scale or severity to be classified as a Serious Incident Requiring Investigation (SIRI) (via the NHS Digital checklist on the DSP Toolkit) will be:

* + - Notified immediately to the CCG’s SIRO and Caldicott Guardian
    - Reported via the Data Security & Protection Toolkit
    - Reported to the Department of Health, Information Commissioners Office and other regulators via STEIS and the HSCIC Incident reporting tool
    - Investigated and reviewed in accordance with the guidance in the HSCIC checklist
    - Reported publicly through the CCGs Annual Report and Governance Statement

## Investigation

The IG Delivery Manager will support the investigation of all IG issues reported. This may include, but is not limited to, breaches of policy, breaches of confidentiality and issues related to IT Security. The IG Delivery Manager will assist with the procedural processes to ensure that investigations of incidents will be carried out in a way that ensures the preservation of evidence and in a manner that enables both legal and disciplinary action to be taken if necessary.

## Organisational Structure for IG Reporting and Assurance

The IGSG has been established to support and drive the broader information governance agenda and provide the Governing Body with the assurance that effective information governance best practice mechanisms are in place within the organisation.

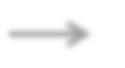
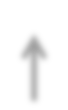
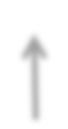
The Group will meet every month and be attended by the SIRO, Head of Governance, Risk Manager and the IG Delivery Manager. See Annex E for the Terms of Reference for this group.

The IGSG will report to the IA&G Committee through minutes or action notes and will ensure the committee is briefed on any significant issues.

The SIRO will ensure that the IA&G Committee receive the minutes of the IGSG and that they are made aware of any IG matters of concern.

The Governing Body retains overall responsibility and accountability for all aspects of Information Governance.

# = Reporting

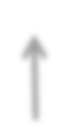


Governing Body

Integrated Audit &

Governance Committee

Information Governance Steering Group



= Assurance

## Policies and Procedures

The Information Governance Framework and Strategy are supported by a range of detailed policies and procedures. These include but are not limited to:

* + Data Protection & Confidentiality Policy
  + Confidentiality: Code of Conduct Policy
  + Records Management policy
  + Safe Haven Policy
  + Remote Access & Home Working Policy
  + Information Security Policy
  + Business Continuity Policy & Plans
  + Confidentiality Audit Policy
  + Subject Access Request Policy
  + Acceptable Computer Use Policy
  + Email Policy
  + IAO role and responsibilities
  + Information Governance Checklist and Privacy Impact Assessment All of these documents are available on the CCG Internet site;

## Reference Material.

* + **Data Protection Act**
  + **General Data Protection Regulation** (GDPR)
  + **Human Rights Act 1998** (Specifically Article 8)
  + **NHS Information Governance**: Guidance on Legal and Professional Obligations.
  + **Report on the Review of Patient-Identifiable Information 1997** (Caldicott Report)
  + **Report of the Caldicott2 Review - Information**: To share or not to share? The Information Governance Review 2013

## Government Response to Report of the Caldicott2 Review 2013.

* + **NHS England: Everyone** Counts: Planning for Patients 2014/15 to 2018/19.
  + **NHS Digital**: A guide to confidentiality in health and social care: Treating confidential information with respect - September 2013
  + **NHS Digital**: A guide to confidentiality in health and social care: references - September 2013
  + **National Information Board and DH**: Personalised Health and Care 2020
  + **NHS England**: NHS Standard Contract
  + **Information Commissioner**: Data Sharing Code of Practice
  + **Information Commissioner**: Privacy Impact Assessment Code of Practice

In addition to the above policies and guidance documents the Registration Authority is managed and run by the IG Provider. Any work in this area will be completed following the Registration Authority Standard available on the IG Provider Portal.

## Annex A

**NORTH LINCOLNSHIRE CCG INFORMATION GOVERNANCE STRATEGY 2019 to 2020**

1. The IG Strategy of NLCCG will be based upon a vision of a long term delivery of clear open principles to ensure that:
   1. The CCG complies with all statutory requirements
   2. The CCG has an information governance strategy that supports the achievement of corporate objectives
   3. The CCG can demonstrate an effective framework for managing information governance assurance
   4. Staff are aware of their responsibilities and the importance of information governance
   5. Information governance becomes a systematic, efficient and effective part of business as usual for the organisation
   6. Information governance is integrated into the change control process
   7. That there are effective methods for seeking assurance across the organisation and with its key partners
   8. That the organisation can demonstrate that the information governance arrangements of organisations it commissions services from across healthcare and commissioning support are adequate
   9. The CCG will facilitate and encourage the sharing of information where it is in the interest of the patients and ensure that any sharing remains compliant with information governance requirements.

## Annex B

**Art. 5 GDPR Principles relating to processing of personal data**

Personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with [Article 89](https://gdpr-info.eu/art-89-gdpr/)(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’);
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with [Article 89(](https://gdpr-info.eu/art-89-gdpr/)1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’);
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).

## Annex C

**Caldicott Principles**

1. **Justify the purpose(s)**

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

1. **Don’t use personal confidential data unless it is absolutely necessary** Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

## Use the minimum necessary personal confidential data

Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

## Access to personal confidential data should be on a strict need-to-know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

## Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling personal confidential data — both clinical and non-clinical staff — are made fully aware of their responsibilities and obligations to respect patient confidentiality.

## Comply with the law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

## The duty to share information can be as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

1. **Inform Patients and Service Users about how their confidential information is used.**

A range of steps should be taken to ensure that there are no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information – in some cases, greater engagement will be required.

## Annex D

**Everyone Counts: Planning for Patients 2014/15 - 2019/20**

This document sets out the NHS England vision with regards to the provision and outcomes of high quality care for all, now and for future generations. One of the six national conditions focuses in on ‘Better data sharing between health and social care, based on the NHS number’ and that local organisations should ‘ensure they have the appropriate Information Governance controls in place for information sharing in line with Caldicott 2, and if not, when they plan for it to be in place.’

The requirements of the above document are as follows:

The CCG should where required

* 1. Confirm that they are using the NHS Number as the primary identifier for health and care services, and if they are not, when they plan to;
  2. Confirm that they are pursuing open APIs (i.e. systems that speak to each other); and
  3. Ensure they have the appropriate Information Governance controls in place for information sharing in line with Caldicott 2, and if not, when they plan for it to be in place.

NHS England has already produced guidance that relates to both of these areas. (It is recognised that progress on this issue will require the resolution of some Information Governance issues by DH).

## Annex E

Description: Description: Description: C:\Documents and Settings\SimpsonV\Desktop\North Lincolnshire CCG col.jpg

**Information Governance Steering Group Terms of Reference**

**Information Governance Sub Group**

**Terms of Reference – January 2021**

1. **Purpose**

The Information Governance Sub Group (IGSG) will be the organisation’s forum with delegated authority to oversee Information Governance issues, assurance and work plans on behalf of the Clinical Commissioning Group (CCG).

**Overall Purpose**

The Information Governance Sub Group is a standing committee accountable to the Integrated Audit & Governance Committee (IA&GC). The group’s purpose is to support and embed the broader information governance agenda within the organisation and provide the Governing Body with assurance that effective information governance is in place within the organisation. The group is responsible for the following areas of work:

* Confidentiality and Consent;
* Data Protection;
* Data Quality;
* Information Management;
* Information Disclosure and Sharing;
* Information Security;
* Records Management;
* Registration Authority;
* Access Control;
* Information Governance Incident Reporting; and
* Freedom of Information.

1. **Accountability**

The Accountable Officer has overall accountability for ensuring that the organisation operates in accordance with statutory requirements as outlined in the Information Governance Management Framework.

The Chair/Vice Chair of the Information Governance Steering Group will provide quarterly reports to the Integrated Audit & Governance Committee for assurance. A report for the Governing Body will be submitted to the Integrated Audit & Governance Committee alongside the organisation’s annual submission of the Data Security & Protection Toolkit (DSPT) for formal sign off and formally authorised by the SIRO prior to submission of the organisation’s end of year toolkit scores.

## Delegated Authority

The IGSG is accountable to theGoverning body through theIntegrated Audit & Governance committee and is authorised to:

* investigate any activity within its terms of reference
* seek any information it requires from any employee and all employees are directed to co-operate with any request made by the Group. This remit extends to those working on any of the statutory bodies’ behalf; and
* co-ordinate and implement activities in line with these terms of reference, as part of the Information Governance work programme.

This group provides assurance to the IA&G committee that robust information governance controls are in place and that there are no material concerns within the CCG in regards to retaining its DSP Toolkit compliance.

1. **Declaration of Interests** 
   1. Declaration of Interests will be a standing agenda item at each meeting. Any changes to interests should be declared in the next possible meeting.
2. **Duties**

The Group is tasked with:

* ensuring organisation-wide engagement in the Information Governance agenda;
* ensuring that the Information Governance Assurance Framework is embedded across the organisation, and
* providing a local forum for Information Governance team leads, disseminating best practice and receiving feedback regarding concerns, issues and problems.

**Specific Responsibilities**

Specific Responsibilities are as follows:

* cascade national guidance and advice;
* lead on local implementation of guidance and advice;
* receive and action Information Governance performance reports produced by provider of information governance to the CCG
* receive and review Information Governance policies and procedures;
* ensuring that agreed information governance strategies, policies and procedures are embedded within the culture and practice of the organisation and adhered to;
* ensuring that local operational leads are assigned for specific areas of the toolkit as appropriate, who will be responsible for providing evidence to support DSP Toolkit compliance and reviewing and approving toolkit scores in their designated area(s); and take forward lessons learned resulting from information governance incidents.
* **Membership**

In order to appropriately discharge DSP Toolkit accountabilities and responsibilities the group should be attended by representation from the following teams. Members should represent the interests of the team.

The core membership of this committee will be as follows:

| **Role** | **Responsible Member** |
| --- | --- |
| Chair | Associate Director of Corporate Affairs |
| Deputy Chair | Risk Manager |
| SIRO/Finance | Senior Information Risk Owner (SIRO)/Chief Finance Officer |
| DPO | Data Protection Officer |
| IG Specialist | Information Governance Delivery Manager |
| Deputy Caldicott Guardian | Deputy Director of Nursing & Quality |
| Corporate Support | Business Manager |

Where a member is unable to attend, a deputy or nominated representative should attend in their place.

1. **Quoracy**

The steering group shall be quorate so long as the Information Governance Delivery Manager and the Chair (or their designated representatives) are present.

1. **Frequency of Meetings**

The IGSG will meet monthly and synchronise with the IA&G committee.

1. **Administration of Meeting**

* the agenda will be managed by the Business Manager and circulated to members at least 3 working days prior to the meeting along with discussion papers;
* agreed actions will be documented and circulated to all members within 7 working days of the meeting;
* electronic copies of all action notes will be maintained on the corporate intranet;
* Action notes will be kept of the proceedings and submitted to the Quality Group

1. **Review of ToRs** 
   1. The Terms of Reference for this group will be reviewed annually and submitted to the IA&G committee for approval.

**For review 31 January 2022**

## Annex F

C:\Documents and Settings\helen.sanderson\Local Settings\Temporary Internet Files\Content.Outlook\6UXB7KOT\NLlogo.png

**Data Protection by Design Audit**

* The GDPR requires you to put in place appropriate technical and organisational measures to implement the data protection principles and safeguard individual rights. This is ‘data protection by design and by default’.
* In essence, this means you have to integrate or ‘bake in’ data protection into your processing activities and business practices, from the design stage right through the lifecycle.
* This concept is not new. Previously known as ‘privacy by design’, it has always been part of data protection law. The key change with the GDPR is that it is now a legal requirement.
* Data protection by design is about considering data protection and privacy issues upfront in everything you do. It can help you ensure that you comply with the GDPR’s fundamental principles and requirements, and forms part of the focus on accountability.

Audit Checklist

* + We consider data protection issues as part of the design and implementation of systems, services, products and business practices.
  + We make data protection an essential component of the core functionality of our processing systems and services.
  + We anticipate risks and privacy-invasive events before they occur, and take steps to prevent harm to individuals.
  + We only process the personal data that we need for our purposes(s), and that we only use the data for those purposes.
  + We ensure that personal data is automatically protected in any IT system, service, product, and/or business practice, so that individuals should not have to take any specific action to protect their privacy.
  + We provide the identity and contact information of those responsible for data protection both within our organisation and to individuals.
  + We adopt a ‘plain language’ policy for any public documents so that individuals easily understand what we are doing with their personal data.
  + We provide individuals with tools so they can determine how we are using their personal data, and whether our policies are being properly enforced.
  + We offer strong privacy defaults, user-friendly options and controls, and respect user preferences.
  + We only use data processors that provide sufficient guarantees of their technical and organisational measures for data protection by design.
  + When we use other systems, services or products in our processing activities, we make sure that we only use those whose designers and manufacturers take data protection issues into account.
  + We use privacy-enhancing technologies (PETs) to assist us in complying with our data protection by design obligations.

Annex G

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **INTEGRATED IMPACT ASSESSMENT** | | | | | | | | |
| Policy/project/function/service | Information Framework & Strategy | | | | | | | |
| Date of analysis: | 16/12/2021 | | | | | | | |
| Type of analysis completed | Quality | | | | Yes | | | |
| Equality | | | | Yes | | | |
| Sustainability | | | | Yes | | | |
| What are the aims and intended effects of this policy/project or function? | Support the CCG's compliance with good practice and national requirements in relation to Information Governance. | | | | | | | |
| Please list any other policies that are related to or referred to as part of this analysis | Data Protection & Confidentiality Policy, Records Management Policy, Information Security Policy, Safe Haven Policy, Business Continuity Policy, Subject access Request Policy, Acceptable Computer Use Policy, E Mail Policy | | | | | | | |
| Who does the policy, project, function or service affect? | Employees | | | | Yes | | | |
| Service users | | | | No (not directly) | | | |
| Members of the public | | | | No | | | |
| Other (please list) | | | | No | | | |
|  | | | | | | | | |
| **QUALITY IMPACT** | | | | | | | | |
|  | **Please ‘X’ ONE for each** | | | **Brief description of potential impact** | | **Mitigation strategy and monitoring arrangements** | **Risk 5 x 5 risk matrix)** | |
| **Chance of Impact on Indicator** | | |
| **Positive Impact** | **No Impact** | **Negative Impact** | **Likelihood** | **Consequence** |
| **X** | **X** | **X** |

Annex G

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **PATIENT SAFTEY** | | | | | | | |
| Patient safety /adverse events | **X** |  |  | **Promotes effective management and security of information**  **and thus patient safety.** |  |  |  |
| Mortality position |  | **X** |  |  |  |  |  |
| Infection control MRSA/CDIFF |  | **X** |  |  |  |  |  |
| CQC status |  | **X** |  |  |  |  |  |
| NHSLA / CNST |  | **X** |  |  |  |  |  |
| Mandatory/statutory training | **X** |  |  | **Supports staff undertaking training in relation to IG/Cyber Security** |  |  |  |
| Workforce (vacancy turnover absence) |  | **X** |  |  |  |  |  |
| Safe environment |  | **X** |  |  |  |  |  |
| Standard & suitability of equipment |  | **X** |  |  |  |  |  |
| **CLINICAL EFFECTIVENESS** | | | | | | | |
| NICE Guidance and National Quality Standards, eg VTE, Stroke, Dementia |  | **X** |  |  |  |  |  |
| Patient related outcome  measures |  | **X** |  |  |  |  |  |
| External accreditation e.g. professional bodies i.e. RCN |  | **X** |  |  |  |  |  |
| CQUIN achievement |  | **X** |  |  |  |  |  |
| **PATIENT EXPERIENCE** | | | | | | | |

Annex G

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Will there be an impact on patient experience if so how |  | **X** |  |  | |  |  |  |
| Will it impact on carers if so how |  | **X** |  |  | |  |  |  |
| **INEQUALITIES OF CARE** | | | | | | | | |
| Will it create / reduce variation in care provision? |  | **X** |  |  | |  |  |  |
| **STAFF EXPERIENCE** | | | | | | | | |
| What is the impact on workforce capability care and skills? |  | **X** |  |  | |  |  |  |
| Will there be a change in working practice, if so, how? |  | **X** |  |  | |  |  |  |
| Will there be an impact on training | **X** |  |  | **Supports staff undertaking training in relation to IG/Cyber Security** | |  |  |  |
| **TARGETS / PERFORMANCE** | | | | | | | | |
| Will it have an impact on performance, if so, how? |  | **X** |  |  | |  |  |  |
| Could it impact on the achievment of local, regional, national targets, if so, how? |  | **X** |  |  | |  |  |  |
|  | | | | | | | | |
| **EQUALITY IMPACT** | | | | | | | | |
| Analysis Rating (see completion notes) | Red |  | Red/Amber |  | Amber |  | Green |  |

Annex G

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Approved by: | Commissioner Lead: |  | GP lead for E&D: |  |
| Date |  | Date |  |
| **Local Profile Data** | | | | |
| General | Not applicable | | | |
| Gender (Men and Women) |  | | | |
| Race (All Racial Groups) |  | | | |
| Disability (Mental and Physical, Sensory Impairment, Autism, Mental Health Issues) |  | | | |
| Religion or Belief |  | | | |
| Sexual Orientation (Heterosexual, Homosexual and Bisexual) |  | | | |
| Pregnancy and Maternity |  | | | |
| Transgender |  | | | |
| Marital Status |  | | | |
| Age |  | | | |
| **Equality Data** | | | | |
| Is any equality data available relating to the use or implementation of this policy, project or function? | N/A | | | |

Annex G

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| List any consultation e.g. with employees, service users, Unions or members of the public that has taken place in the development or implementation of this policy, project or function. | N/A | | | |
| Promoting inclusivity; How does the project, service or function contribute to our aims of eliminating discrimination and promoting equality and diversity? | N/A | | | |
| **Equality Impact Risk Assessment test** | | | | |
| What impact will the implementation of this policy, project or function have on employees, service users or other people who share characteristics protected by *The Equality Act 2010*? | | | | |
| Protected Characteristic: | No Impact | Positive Impact | Negative Impact | Evidence of impact and if applicable justification where a *Genuine Determining Reason* exists |
| Gender (Men and Women) | X |  |  |  |
| Race (All Racial Groups) | X |  |  |  |
| Disability (Mental and Physical, Sensory Impairment, Autism, Mental Health Issues) | X |  |  |  |
| Religion or Belief | X |  |  |  |
| Sexual Orientation (Heterosexual, Homosexual and Bisexual) | X |  |  |  |
| Pregnancy and Maternity | X |  |  |  |

Annex G

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Transgender | X |  |  |  | | | |
| Marital Status | X |  |  |  | | | |
| Age | X |  |  |  | | | |
| **Action Planning** | | | | | | | |
| As a result of performing this Equality Impact Analysis, what actions are proposed to remove or reduce any risks of adverse outcomes identified on employees, service users or other people who share characteristics protected by The Equality Act 2010? | | | | | | | |
| Identified Risk: | | Recommended Action: | | | Responsible Lead | Completion Date | Review Date |
|  | |  | | |  |  |  |
|  | |  | | |  |  |  |
|  | |  | | |  |  |  |
| **SUSTAINABILITY IMPACT** | | | | | | | |
| Staff preparing a Policy / Board Report / Committee Report / Service Plan / Project are required to complete a Sustainability Impact Assessment.  Sustainability is one of the Trust’s key Strategies and the Trust has made a corporate commitment to address the environmental effects of activities across Trust services. The purpose of this Sustainability Impact Assessment is to record any positive or negative impacts that this activity is likely to have on each of the Trust’s Sustainability Themes. | | | | | | | |
|  | | **Positive Impact** | **Negative Impact** | **No Specific**  **Impact** | **What will the impact be? If the impact is negative, how can it be mitigated? (action)** | | |
| Reduce Carbon Emission from buildings by 12.5% by 2010-11 then 30% by 2020 | |  |  | X |  | | |

Annex G

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| New builds and refurbishments over £2million (capital costs) comply with BREEAM Healthcare requirements. |  |  | X |  |
| Reduce the risk of pollution and avoid any breaches in legislation. |  |  | X |  |
| Goods and services are procured more  sustainability. |  |  | X |  |
| Reduce carbon emissions from road vehicles. |  |  | X |  |
| Reduce water consumption by 25% by 2020. |  |  | X |  |
| Ensure legal compliance with waste legislation. |  |  | X |  |
| Reduce the amount of waste produced by 5% by 2010 and by 25% by 2020 |  |  | X |  |
| Increase the amount of waste being recycled to 40%. |  |  | X |  |
| Sustainability training and communications for employees. |  |  | X |  |
| Partnership working with local groups and organisations to support sustainable development. |  |  | X |  |
| Financial aspects of sustainable development are considered in line with policy requirements and  commitments. |  |  | X |  |