Humber and North Yorkshire Health and Care Partnership

NHS Humber and North Yorkshire Integrated Care Board (ICB)

Agenda Item No:	17i

Report to:	Humber and North Yorkshire Integrated Care Board
Date of Meeting:	10 January 2023
Subject:	**Information Governance Framework**
Director Sponsor:	Karina Ellis – Executive Director of Corporate Affairs
Author:	Hayley Gillingwater – Senior Information Governance Manager

STATUS OF THE REPORT:

Approve ☒ Discuss ☐ Assurance ☐ Information ☐ A Regulatory Requirement ☐

SUMMARY OF REPORT:

As per the requirements of the Data Security and Protection Toolkit the ICB must demonstrate that we have clear documented lines of accountability and responsibility to named individuals in relation to Information Governance.

The purpose of this policy is to establish clear guidelines and accountability in relation to Information Governance to protect personal data.

It is important to note that this framework is not exhaustive and may need to be adapted and updated periodically as the organisation and regulatory requirements evolve.

RECOMMENDATIONS:

Members are asked to:

i) Approve this policy.

ICB STRATEGIC OBJECTIVE

Managing Today	☒
Managing Tomorrow	☒
Enabling the Effective Operation of the Organisation	☒

IMPLICATIONS	
Finance	N/A
Quality	N/A
HR	N/A
Legal / Regulatory	Complies with requirements of Data Protection Legislation.
Data Protection / IG	Complies with requirements of Data Protection Legislation.
Health inequality / equality	N/A
Conflict of Interest Aspects	N/A
Sustainability	A Sustainability Impact Assessment has been undertaken. No positive or negative impacts were identified against the twelve sustainability themes.

ASSESSED RISK:

No risks identified.

MONITORING AND ASSURANCE:

Not applicable – just seeking approval of policy.

ENGAGEMENT:

Feedback and engagement was sought from Governance colleagues and members of the ICB Information Governance Group.

REPORT EXEMPT FROM PUBLIC DISCLOSURE No ☒ Yes ☐

If yes, please detail the specific grounds for exemption.

Humber and North Yorkshire
Health and Care Partnership

NHS
Humber and
North Yorkshire
Integrated Care Board (ICB)

Information Governance Framework
December 2023

Authorship:	Senior Information Governance Manager – Humber & North Yorkshire Integrated Care Board
Committee Approved:	ICB Board
Approved date:	Month/ year
Equality Impact Assessment:	Month/ year
Target Audience:	ICB and its Committees and Sub-Committees, ICB Staff, agency and temporary staff & third parties under contract
Policy Number:	ICB 59
Version Number:	1.0

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.

AMENDMENTS

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

New Version Number	Issued by	Nature of Amendment	Approving body	Approval date	Date published on website
1.0	Executive Director of Corporate Affairs	New Policy	ICB Board	TBC	TBC

Contents

1 Introduction

This policy sets out the approach to be taken within the ICB to provide a robust Information Governance Framework and to fulfil its overall objectives. Information Governance requirements ensure that best practice is implemented and on-going awareness is evidenced across the ICB. The ICB is committed to ensuring that all records and information are dealt with legally, securely, efficiently and effectively.

Information Governance is a "framework for handling information in a confidential and secure manner to appropriate ethical and quality standards in modern health services".
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.

2 Purpose

The purpose of this framework is to describe the management arrangements to deliver Information Governance (IG) assurance across Humber & North Yorkshire Integrated Care Board (H&NY ICB) and to provide guidance on compliance with the UK General Data Protection Regulation, the Data Protection Act 2018 and the Common Law Duty of Confidentiality. 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.

This policy will 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 H&NY ICB maintains high standards of IG.

The ICB will establish, implement, and maintain procedures linked to this policy to ensure compliance with the requirements of data protection legislation, records management, information security and other related legislation and guidance, contractual responsibilities and to support the assurance standards of the Data Security and Protection Toolkit.

3 Definition/ Explanation of Terms

Corporate Information - A corporate record is a record of activity within the ICB. This will include both information collected for business purposes and information created within the ICB, the processing of that information and reports produced from that information. Where this does not contain and is not linked to personal information no legal basis need be identified to process the information. However, the ICB will need to consider whether this information is to be published into the public domain or whether it is corporately sensitive and implement controls to manage it appropriately.

Data Breach - A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

Data Controller - A natural or legal person, public authority, agency or other body alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor - A natural or legal person, public authority, agency or other body which processes data on behalf of the controller.

Personal Information - Person-identifiable information is anything that contains the means to identify a person, e.g., name, address, postcode, date of birth, NHS number, National Insurance number, pseudonymised data, online identifiers and location data, etc. Any data or combination of data and other information, which can indirectly identify a person, will also fall into this definition.
Whenever possible, anonymised data, that is data where all personal details have been removed and which therefore cannot identify the individual, should be used. Note however that even anonymised information can only be used for justified purposes.
Information that identifies individuals personally must be regarded as confidential and should not be used unless absolutely necessary. The appropriate legal basis under Article 6 of the General Data Protection Regulation must be identified and recorded in the ICB or Place Information Asset Register to comply with data protection legislation.

Processing - in relation to information or data means; obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, which may include adaptation or alteration of the information; retrieval, or use of the information or data; disclosure of the information or data by transmission, dissemination or otherwise making available, or alignment, combination, blocking, erasure or destruction of the information or data. In summary anything you do with data is “processing”.

Special Category Data – also known as sensitive data includes, Health Data, Trade Union membership, Political opinions, Religious or philosophical beliefs, Racial or Ethnic Origin, Sex life and sexual orientation, Biometric Data and Genetic Data.

In addition to having identified a legal basis under Article 6 of the General Data Protection Regulation to legally process personal identifiable information, to legally process special category information the ICB must identify the condition under Schedule 1 of the current Data Protection Act and the legal basis under Article 9(2) and record these on the relevant Information Asset Register.

4 Scope of the Policy

The policy applies to NHS Humber and North Yorkshire and all its employees and must be followed by all those who work for the organisation, including the Integrated Care Board, Integrated Care Partnership, those on temporary or honorary contracts, secondments, pool staff, contractors and students.

Non-compliance with this Policy may result in disciplinary action and in extreme cases dismissal.

5 Duties/ Accountabilities and Responsibilities

5.1 Caldicott Guardian

The Caldicott Guardian for the ICB is the Executive Director Clinical and Care Professional. There are also Deputy Caldicott Guardians at Place; usually Place Nurse Directors/ Directors of Nursing.

The Caldicott Guardian is a senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate and secure information-sharing. The Guardian(s) plays a key role in ensuring that NHS, Councils with Social Services responsibilities, 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.

5.2 Senior Information Risk Owner (SIRO)

The SIRO for the ICB is the Executive Director of Corporate Affairs. There are also Deputy SIROs at Place; usually the Place Director of Finance.

The Senior Information Risk Owner (SIRO) will take overall ownership of the organisation's information risks, act as champion for information risk on the Board and provide written advice to the Chief Executive 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.

5.3 Data Protection Officer (DPO)

The ICB's Data Protection Officer is the Director of Governance and Board Secretary. There are also Deputies at some Places; usually DPOs from the local Councils. The role of Data Protection Officer is to facilitate the ICBs compliance with data protection legislation. The DPO will:

- Monitor ICB compliance with the data protection responsibilities and obligations.
- Provide advice and assistance with regards to the completion of Data Protection Impact Assessments
- Act as a contact point for the Information Commissioners Office (ICO), members of the public and ICB staff on matters relating to data protection.
- Assist in implementing essential elements of the data protection legislation such as the principles of data processing, data subjects' rights, data protection impact assessments, records of processing activities, security of processing and notification and communication of data breaches.

5.4 Senior Information Governance Manager

The Senior IG Manager supports the DPO and is responsible for the co-ordination of the implementation of systems within the ICB. The Senior IG Manager is accountable for ensuring effective management, accountability, compliance and assurance for all aspects of IG across the ICB. This role includes but is not limited to:

- developing and maintaining comprehensive and appropriate documentation that demonstrates commitment to and ownership of IG responsibilities,
- 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.
- Provide advice and assistance with regards to the completion of Data Protection Impact Assessments
- Assess data breaches and communicate follow up actions to staff.
- Act as a contact point for the Information Commissioners Office (ICO), members of the public and ICB staff on matters relating to data protection.
- Assist in implementing essential elements of the data protection legislation such as the principles of data processing, data subjects' rights, data protection impact assessments, records of processing activities, security of processing and notification and communication of data breaches.

5.5 Information Asset Owners & Administrators (IAOs & IAAs)

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 where appropriate.

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

5.6 Line Mangers

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.

5.7 All staff

All members of staff have a responsibility to ensure they are aware of all data protection, information security policies and guidance and comply with them. 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 must be reported immediately via the desktop incident reporting portal. Depending on the circumstances this may be considered a disciplinary offence which could result in dismissal or termination of employment contract. Staff must be aware of their personal responsibility for the security and confidentiality of information which they use.

All staff are responsible for compliance with data protection legislation.

5.8 Third Party Providers/ Suppliers/ Contractors

The ICB must conduct due diligence on third party providers/ suppliers or contractors providing services to and on behalf of the ICB. Contracts with third parties providing services must include appropriate, detailed and explicit requirements regarding confidentiality, data protection and information governance to ensure that Contractors are aware of IG obligations.

All support services that process information for or on behalf of the ICB will be required to:

- Assist with the completion of data protection impact assessments if the third party is processing personal and or sensitive information.

- 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 ICB.

- Ensure that services commissioned meet the requirements of the current data protection legislation 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 processing patient data), and at the request of the ICB, 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 ICB.

- 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 of services or decommission of service e.g. passing on data/deletion/retention of data at the end of the contract.

Responsibilities for approval

The Integrated Care Board is responsible for the review and approval of this policy.

6 Humber & North Yorkshire Information Governance.

6.1 Data Protection Act 2018

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR) and is the most fundamental piece of legislation that underpins Information Governance. The ICB are registered with the Information Commissioners Office and will fully comply with all legal requirements. A process will be adopted to promote Privacy by Design and ensure that a review of all new systems is carried out and where requirements such as the need for Data Protection Impact Assessments (DPIA) are highlighted these will be completed.

6.2 Data Security & 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 complete the toolkit to a satisfactory level. Annual plans will be developed year on year from the DSPT to achieve the required standard. As the DSPT is a publicly available assessment, the scores of partner organisations will be used to assess their suitability to share information and to conduct business with.

6.3 Caldicott Principles & 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 are two reports that have identified specific principles that are considered essential practice for the appropriate sharing and security of Patient Information.

The Government Response to 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 apply to the use of confidential information within health and social care organisations and when such information is shared with other organisations and between individuals, both for individual care and for other purposes.

The principles are intended to apply to all data collected for the provision of health and social care services where patients and service users can be identified and would expect that it will be kept private. This may include for instance, details about symptoms, diagnosis, treatment, names and addresses. In some instances, the principles should also be applied to the processing of staff information.

The Caldicott Principles can be found at: The Caldicott Principles - GOV.UK (www.gov.uk)

6.4 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.

6.5 Accreditation of Information Systems

- The ICB shall ensure that all new information systems, applications and networks include a security policy are appropriately approved prior to implementation.

- System level security policies must be developed for systems under ICB control in order to allow granularity in the security management considerations and requirements of each. This may result in specific responsibilities being assigned and obligations communicated directly to those who use the system.

- The ICB shall ensure that all new information systems, applications and networks include a Data Protection Impact Assessment (DPIA) and System Level Security Policy (SLSP) and are approved by the Senior Information Governance Manager, DPO and SIRO or Caldicott Guardian and the ICB's IT Service providers before they commence operation.

- When planning for, and during procurement of, new systems, it is the responsibility of the Project Manager or Lead to ensure that appropriate system security features are included within the system. As a minimum this will include a password protection feature and audit logs.

    - Systems and applications must be adequate for their purpose.

    - Software applications, upgrades and amendments must be developed in a controlled manner, documented and thoroughly tested before implementation.

    - Unauthorised software must not be introduced onto any system without prior authorisation from the ICB's IT Service Providers.

6.6 Handling Confidential Information

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

In addition the ICB must have arrangements in place to ensure:

- That data subjects are appropriately informed of all uses of their information.
- Data Protection Impact Assessments (DPIAs) are completed for new commissioning activities, projects, systems or when undertaking work that requires the processing of personal data.
- The security of information at all points of its lifecycle.
- There is a process to recognise and record objections to the handling of confidential information and the circumstances under which an objection cannot be upheld.
- That if objections are received where the proposed uses of information are not required by law, the ICB should ensure they act in accordance with that objection.
- Procedures are implemented for recognising and responding to individuals' requests for access to their personal information.
- Appropriate information sharing arrangements are in place.
- Appropriate data processing agreements are in place to collect or obtain information for management purposes.
- Staff are appropriately trained to handle confidential information.
- Staff are aware of and follow data breach reporting processes.

The Health & Social Care Information Centre (HSCIC) 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.

6.7 Openness & Transparency

- The ICB recognises 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 organisation 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 ICB 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 organisational

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 ICB 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 ICB's subject access request policy.

- The ICB will have clear procedures and arrangements for liaison with the press and broadcasting media.

6.8 Legal Compliance

- The ICB regards all identifiable personal information relating to patients as confidential. Compliance with legal and regulatory requirements will be achieved, monitored and maintained.

- The ICB 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 ICB will undertake or commission annual assessments and audits of its compliance with legal requirements as part of the annual assessment against the Data Security and Protection Toolkit assertions and in line with changes and developments in legislation and guidance.

- The ICB 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 Duty of Confidentiality and associated guidance

- The ICB 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.

6.9 Data Breaches/ Incident Management

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 ICB's Desktop Incident Reporting Portal in line with the Incident Management Policy. Under data protection legislation where a data breach is likely to result in a risk to the rights and freedoms of the individual, this must be reported to the Information Commissioners Office within 72 hours. Therefore, all breaches must be reported as soon as staff become aware to enable the Senior Information Governance Manager to

investigate the incident, assess the risk and where required report the incident to the ICO within the required timescale.

An information governance incident of sufficient scale or severity will be:

- Notified immediately to the ICB's SIRO DPO and Caldicott Guardian.
- Reported via the Data Security & Protection Toolkit.
- Reported to the Department of Health, Information Commissioners Office and other regulators as necessary.
- Reported publicly through the ICB's Annual Report and Governance Statement.

6.10 Investigation

All incidents reported via the desktop portal will be investigated by the Senior Information Governance Manager or Information Governance Officers with support from the Data Protection Officer, Senior Information Risk Owner and the Caldicott Guardian as appropriate.

If necessary, the ICB's IT providers 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 Team 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.

6.11 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, with support from Information Asset Owners will be responsible for assessing any risks associated with specific data processing. The IG Team will recommend controls to reduce risks where necessary. Any information flows from or into identified information assets will be risk assessed and the results reported to the ICB SIRO for risk mitigation, acceptance or transfer.

Risks that cannot be mitigated but are accepted by the ICB will be added to the relevant risk register and managed in accordance with the Risk Management Policy.

6.12 Organisational Structure for Reporting & Assurance

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

The Board 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 assurance updates/reports from the Audit Committee or the Senior Information Risk Owner. The Audit Committee will receive and annual report from the Senior Information Risk Owner.

The ICB Strategic Information Governance Group has been established to support and drive the broader information governance agenda and provide the Audit Committee and

the ICB Board with the assurance that effective information governance best practice mechanisms are in place within the organisation.

An operational Information Governance Steering Group has been established with representation from each Place.

The below table illustrates responsibilities of the Operational Information Governance Group and the responsibilities of the ICB Strategic Information Governance Group.

Operational level	ICB Strategic Level
Support development and implement ICB IG policies and procedures: • Review DPIAs and recommend sign-off for ICB wide DPIAs if appropriate • Review ISAs and recommend for ICB sign-off • Sign-off Place destruction logs • Provide advice and guidance at a local level e.g. SARs, data breaches etc. • Approval of one-off requests for access to clinical systems • Monitor local IG action plan and risks • Review data breaches/ incidents • Undertake specialist training in line with requirements of TNA. • Conduct building spot checks • Maintain Information Asset Registers and data flow maps • Coordinate DSPT evidence gathering	Deliver statutory function supported by wider expertise from across the ICB: • Co-ordinate IG functions • Provide ICB IG policies and procedures • Coordinate DSPT • Coordinate audits and assessments • Produce and review Privacy notices • ICO investigations • Compliance monitoring and reporting • IG reporting • Sign-off ISAs and ICB wide DPIAs • Provide advice and guidance • Ensure sufficient IG capacity to support the ICB • Undertake specialist training in line with requirements of TNA. • Ensure ICB and relevant staff are registered with ICO and NHSE/I

7 Consultation

All stakeholders such as ICB SIRO/DPO and Executive lead and IG leads involved in developing, implementing, managing, and monitoring data protection and confidentiality have been engaged in the development of this policy.

8 Training

Training and education are key to the successful implementation of this framework and strategy and embedding a culture of IG management in the organisation. Staff will have the opportunity to develop more detailed knowledge and appreciation of the role of IG through:

- Policy/strategy
- Induction
- Line manager
- Specific training courses
- Statutory and Mandatory training workshops
- Information Asset Administrator and Information Asset Owner workshops
- Data Protection Impact Assessment training workshops
- Communications/updates from the IG Lead
- The IG Handbook

Mandatory training sessions will be delivered online via the Electronic Self-Service (ESR) portal; Data Security Level 1 e-learning package. These sessions are mandatory and must be completed within 7 days for new starters and annually for all staff. Data Security Standard 3 within the Caldicott 3 review requires that all staff undertake appropriate annual data security training and pass a mandatory test. Therefore, non-permanent staff must also complete annual training.

Awareness will be monitored via regular checks and gaps in knowledge will be addressed via further bespoke training materials and/or targeted training sessions provided by the IG Team.

The SIRO, DPO and Caldicott Guardian are required to complete additional training relevant to their roles and responsibilities.

Additional Information Governance training such as Information Asset Owner Training and Data Protection Impact Assessment Training is identified in the Information Governance training needs analysis.

9 Monitoring Compliance

- Compliance with this policy will be monitored via the submission and independent audit of the Data Security & Protection Toolkit (DSPT).
- An action plan for improving and implementing the requirements of the DSPT will be submitted to the ICB's Information Governance Group annually.
- The ICB's progress will be reported to the ICB Information Governance Group and the SIRO at regular intervals by the Senior Information Governance Manager.
- The ICB will comply with the NHS' deadlines for submission of updates and the final data security and protection toolkit assessment.
- Annual IG performance will be summarised in the Information Governance Annual Report.
- An internal audit of the DSPT will be undertaken annually in quarter 1 of the financial year as part of the ICB's internal audit plan.

10 Arrangements for Review

This policy will be reviewed every 2 years. Earlier review may be required in response to exceptional circumstances, organisational change, or relevant changes in legislation/guidance, as instructed by the Executive Director responsible for this policy.

11 Dissemination

The policy will be disseminated by being made available on the ICB website and highlighted to staff through staff communications, and by managers.

Breaches of this policy may be investigated and may result in the matter being treated as a disciplinary offence under the HNY ICB's disciplinary procedure.

12 Associated Documentation

- Data Protection & Confidentiality Policy
- IT & Information Security Policies
- Privacy by Design
- Data Protection Impact Assessment Procedure
- Subject Access Request
- Information Governance Staff Handbook
- Incident Policy

This list is not exhaustive.

13 References

- **Data Protection Act 2018**
- **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.**
- **HSCIC**: A guide to confidentiality in health and social care: Treating confidential information with respect - September 2013
- **HSCIC**: A guide to confidentiality in health and social care: references - September 2013
- **NHS England**: NHS Standard Contract
- **Information Commissioner**: Data Sharing Code of Practice
- **Information Commissioner**: Data Protection Impact Assessments (DPIAs)

14 Appendices

Appendix 1 - Anti-Fraud, Bribery and Corruption

15 Impact Assessments

15.1 Equality

NHS Humber and North Yorkshire ICB is committed to creating an environment where everyone is treated equitably and the potential for discrimination is identified and mitigated. It aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others.

An EQIA has been completed and as a result of performing the analysis, the policy does not appear to have any adverse effects on people who share Protected Characteristics.

15.2 Bribery Act 2010

Due consideration has been given to the Bribery Act 2010 in the development of this policy document, further details can be found in appendix 1.

15.3 General Data Protection Regulations (GDPR)

The UK General Data Protection Regulation (GDPR)/ Data Protection Act 2018 includes the requirement to complete a Data Protection Impact Assessment for any processing that is likely to result in a high risk to individuals. Consideration should be given to any impact the policy may have on individual privacy; please consult NHS Humber and North Yorkshire ICB Data Protection Impact Assessment Policy. If you are commissioning a project or undertaking work that requires the processing of personal data, you must complete a Data Protection Impact Assessment.

The ICB is committed to ensuring that all personal information is managed in accordance with current data protection legislation, professional codes of practice and records management and confidentiality guidance. More detailed information can be found in the Data Protection & Confidentiality Policy and related policies and procedures.

Appendix 1 - Anti-Fraud, Bribery and Corruption

The ICB 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 ICB, 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.

To raise any suspicions of bribery and/or corruption please contact the Executive Director of Finance and Investment. Staff may also contact the Local Counter Fraud Specialist (LCFS) at – Audit Yorkshire, email: nikki.cooper1@nhs.net or mobile 07872 988939.

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

If staff prefer, they may call the NHS Counter Fraud reporting line on 0800 028 40 60 between 8am-6pm Monday-Friday or report online at www.reportnhsfraud.nhs.uk. This would be the suggested contact if there is a concern that the LCFS or the Executive Director of Finance and Investment themselves may be implicated in suspected fraud, bribery or corruption.