NHS
Yorkshire
Ambulance Service
NHS Trust

Information Governance Framework

Document Author: Head of Risk and Assurance

Date Approved: May 2021

Document Reference	FW – Information Governance Framework
Version	V1.0
Responsible Committee	Trust Management Group
Responsible Director	Executive Director Quality, Governance and Performance Assurance, Deputy Chief Executive
Document Author	Head of Risk and Assurance
Approved By	Trust Management Group
Date Approved	May 2021
Review Date	May 2023
Equality Impact Assessed (EIA)	Yes – Screening
Protective Marking	Not protectively marked

Document Control Information

Version	Date	Author	Status (A/D)	Description of Change
0.1	Feb 2021	Head of Risk and Assurance	D	Replaced Information Governance Strategy and Information Governance Policy with an Information Governance Framework
1.0	May 2021	Risk Team	A	Approved at TMG
A = Approved D = Draft				
Document Author = Head of Risk and Assurance				
Associated Documentation: Data Protection Policy Information Sharing Policy Records Management Policy Data Quality Policy Disclosure Policy Freedom of Information Policy Risk Management Policy ICT Security Policy and Associated Procedures Email Policy Internet Policy and Procedure Social Media Policy Safety and Security Policy Incident and Serious Incident Management Policy CCTV Policy Safeguarding Policy Disciplinary Policy and Procedure YAS Code of Conduct				

Section	Contents	Page No.
	Staff Summary	5
1	Introduction	6
2	Purpose/Scope	6
3	Strategic Objectives	6
4	Principles	7
5	Training Expectations for Staff	11
6	Implementation Plan	11
7	Monitoring Compliance with this Framework	11
8	Legislation and Guidance	12
9	Appendices	13
	Appendix A - Definitions	13
	Appendix B - Roles & Responsibilities	14

Staff Summary

Information governance plays a key part in supporting clinical governance, service planning and performance management. It also gives assurance to Yorkshire Ambulance Service NHS Trust and to individuals that information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible care and to meet the Trust's legal and good practice responsibilities.
The purpose of this framework is to inform all Trust staff of their responsibility for ensuring that corporate, patient and staff information is safeguarded and used appropriately within the Trust.
The Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information.
The Trust believes that accurate, timely and relevant information is essential to deliver the highest quality health care.
There are clearly defined corporate and managerial responsibilities for information governance across the Trust.
The Trust has a corporate Records Management Policy that is embedded throughout the Trust through effective training and ongoing professional development
The key legislation the Trust muts comply with includes the Data Protection Act 2018, the General Data Protection Regulation 2016, the Freedom of Information (FOI) Act 2000 and the Human Rights Act 1998.
Information security covers the policies and procedures in place to protect information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction.
Information sharing covers the proper governance of information sharing practice across the Trust.
Staff and patients need to be able to trust the validity and authority of information, and have confidence that it is up-to-date and accurate.

1.0 Introduction

1.1 Information governance provides a framework for bringing together all of the requirements, standards and best practice that apply to the handling of information. It is about records management, compliance and also about efficient ways of handling information.

1.3 Yorkshire Ambulance Service NHS Trust recognises the importance of reliable information, both in terms of the clinical management of individual patients and the efficient management of services and resources.

1.4 Information governance plays a key part in supporting clinical governance, service planning and performance management. It also gives assurance to Yorkshire Ambulance Service NHS Trust and to individuals that information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible care and to meet the Trust's legal and good practice responsibilities.

2.0 Purpose/Scope

2.1 The purpose of this framework is to inform all Trust staff of their responsibility for ensuring that corporate, patient and staff information is safeguarded and used appropriately within the Trust.

2.2 All aspects of handling information are covered by this framework, including paper and electronic structured record systems and the transmission of information via communication methods such as email, post and telephone.

2.3 This framework covers all systems utilised by the Trust and any individual employed, in any capacity, by the Trust or working in a voluntary capacity.

3.0 Strategic Objectives

3.1.1 The Trust's information governance objectives are to:

- Comply with all information governance related legislation;
- Establish, implement and maintain policies for the effective management of information;
- Ensure a consistent approach within the NHS with regard to information management;
- Recognise the need for an appropriate balance between openness and confidentiality in the management and use of information;
- Ensure all Trust staff follow and promote best practice;
- Ensure maintenance or year on year improvement with the Data Security and Protection Toolkit (DSPT) assessment;
- Develop an Information Governance culture throughout the Trust;
- Help staff to manage personal information for the benefit of patient care;

- Reduce duplication and look at new ways of working effectively and efficiently;
- Minimise the risk of breaches of personal data;
- Minimise inappropriate uses of personal data.

4.0 Principles

4.1 The Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information.

4.2 The Trust fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard personal information about patients, staff and commercially sensitive information.

4.3 The Trust also recognises the need to share patient information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and in some circumstances, the interests of the public.

4.4 The Trust believes that accurate, timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of all clinicians and managers to ensure and promote the quality of information and to actively use information in decision making processes.

4.5 The Framework is structured around six areas of information governance:

- Information Governance Management;
- Records Management;
- Information Legal Compliance;
- Information Security;
- Information Sharing;
- Data Quality and Assurance.

4.6 **Information Governance Management**

This covers the management of information governance at a corporate, managerial and operational level across the Trust. It will provide the necessary ownership and advocacy functions that can be used to ensure the promotion, development and implementation of thr appropriate information governance infrastructure is delivered across the Trust.

- The Trust has established an Information Governance Working Group (IGWG), comprising of Information Asset Owners (IAOs) from all areas of the Trust, with agreed Terms of Reference who will meet regularly to support and drive the information governance agenda within the Trust;
- The Trust has an approved Information Governance Framework (IGF) and this is embedded across the Trust through effective training and continuing professional development;

- The Trust has an Information Asset Register (IAR) with IAOs assigned to each asset;
- There are clearly defined corporate and managerial responsibilities for information governance across the Trust. The Information Governance Team are responsible for corporate information governance strategy and development, a Senior Information Risk Owner (SIRO) has been appointed, and IAOs/members of the IGWG act as key contacts throughout the Trust;
- Staff training programmes and induction procedures across the Trust effectively raise the awareness of information governance and outline the individual responsibilities contained therein;
- The currency of the IGF is ensured through regular reviews, including monitoring of changes to relevant legislation.

4.7 Records Management

Records management covers the process of creating, describing, using, storing, archiving and disposing of organisational records according to a defined set of standards (usually adherence to ISO 15489). It ensures the Trust's adherence to compliance rules and statutory access requirements as well as protecting an organisation's corporate memoru for re-use.

- The Trust has a corporate Records Management Policy that is embedded throughout the Trust through effective training and ongoing professional development;
- The Trust will implement a corporate file plan to ensure effective electronic records management;
- The Trust will implement a Retention Schedule, covering all company records;
- The Trust will implement a procedure for access and permission control;
- Naming conventions should be developed and embedded within electronic document and records management to assist with filing and retrieval.

4.8 Information Legal Compliance

Compliance covers the legal framework and the standards that need to be established to ensure information management is within the law. The Trust must deal with information lawfully and ethincally. Failure to do so could increase the risk of loss of reputation and litigation. The key legislation the Trust muts comply with includes the Data Protection Act 2018, the General Data Protection Regulation 2016, the Freedom of Information (FOI) Act 2000 and the Human Rights Act 1998.

- The Trust has an approved and monitored Freedom of Information Policy which sets out corporate procedures, roles and responsibilities;

- The Legal Services Department is responsible for managing and monitoring these requests, and IAOs will make sure these requests are processed efficiently within their teams;
- The Trust will apply the public interest test when dealing with FOI requests with qualified exemptions to ensure they are dealt with in a consistent and transparent manner;
- All staff are aware and trained in the various rights of access to information and how these can be exercised inclusively;
- The public are made aware of their information rights and how to exercise them;
- Staff to ensure that information is provided in the most appropriately accessible format within statutory timescales;
- The Information Governance Team will consider appeals to withhold information under the Freedom of Information Act;
- The Trust maintains and regularly reviews a Publication Scheme required under the Freedom of Information Act;
- Personal information is processed in a manner compliant with the data protection principles;
- Intellectual property rights (e.g. copyright) are observed;
- All staff are made aware of and abide by their obligations under the Common Law Duty of Confidentiality.

4.9 Information Security

Information security covers the policies and procedures in place to protect information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction. It will ensure the Trust is able to protect the confidentiality, integrity and availability of information.

- There is an ICT Security Policy in place based on ISO 270001;
- Roles and responsibilities for adherence to the policy are clearly defined and an appropriate training and development programme is in place;
- Security requriements are included in formal system acquisition, development and maintenance procedures;
- Formal procedures are in place to avoid breaches of the law, statutory, regulatory or contractual obligations, and of any security requirements;
- There are policies and procedures to report information security incidents and weaknesses and to escalate action on dealing with these;
- There is a business continuity management process designed to limit the impact of, and recover from, the loss of information assets;
- All changes to information processes are planned and implementation is effectively managed;
- There are controls in place for managing third party access to Trust information systems;

- There are appropriate physical security controls in place to protect information assets;
- Networks are adequately managed and controlled to protecxt them from threats. Security is provided for the systems and applications using the network.

4.10 Information Sharing

Information sharing covers the proper governance of information sharing practice across the Trust. Ensuring that the Trust's practice is of the highest standard, meeting with regulatory mechanisms such as the Data Protection Act 2018 and the Human Rights Act 1998, together with the Common Law Duty of Confidentiality, it is essential in order to imbue confidence amongst those whose personal information is involved in such business processes.

- There is an agreed information sharing agreement (ISA) in place between external organisations setting out principles, operational procedures and key legislative considerations together with practical user guidance;
- The Trust has an Information Sharing Policy in place that's sets out the standards for information sharing;
- All ISAs are completed in full detail setting out in particular the legal justification for each sharing exercise;
- The Information Governance Team are able to give guidance on legal issues in relation to justification for information sharing;
- All ISAs are centrally logged with the Information Governance Team;
- All ISAs are reviewed in the month prior to expiration to ensure continued validity;
- A mechanism for reporting breaches of the agreement is documented, agreed and in place for both internal and external parties;
- A mechanism for monitoring the operation and effectiveness of the agreement is documented, agreed and in place;
- Service areas will, on request, provide assurances that agreed procedures and practice are being followed;
- Information sharing is covered in information governance training for all staff;
- Information sharing is covered as part of information governance awareness during the staff induction process.

4.11 Data Quality

This set of requirements covers the need to ensure the quality and accuracy of the information held by the Trust. Staff and patients need to be able to trust the validity and authority of information, and have confidence that it is up-to-date and accurate. It is important that the Trust is able to measure the level of quality of its information resources and ensure they comply with relevant standards.

- The Trust has an agreed Data Quality Policy;
- Suitable training and development programmes are in place to ensure that staff understand their responsibilities in relation to data quality;
- There is a business continuity plan in place for all systems;
- ISAs include standards for the quality of data being shared with and from the Trust;
- There are metrics in place to assess and monitor the quality of data in business critical systems.

5.0 Training Expectations for Staff

5.1 Training is delivered as specified within the Trust Training Needs Analysis (TNA).

6.0 Implementation Plan

6.1 The latest approved version of this strategy will be posted on the Trust Intranet site for all members of staff to view. New members of staff will be signposted to how to find and access this strategy during Trust Induction.

7.0 Monitoring Compliance with this Framework

7.1 To be assured that this Framework is being implemented, key elements will be monitored for compliance.

- **Compliance against the National Data Guardian’s 10 Data Security Standards through the completion of the Data Security and Protection Toolkit (DSPT) online self-assessment tool.**
  The Quality Committee will monitor overall progress through receipt of quarterly reports. The IGWG will monitor operational progress throughout the year and take action to address any concerns, and deficiencies will be noted and reviewed at subsequent meetings. Individual DSPT leads will additionally monitor operational progress throughout the year.

- **All staff receive annual training and a competency test in information governance.**
  The Quality Committee will monitor progress through receipt of quarterly Information Governance reports.

- **All IAOs trained in their role and undertaking risk reviews of information assets they are responsible for. New information assets will be identified through this review process.**
  Quality Committee will monitor progress through receipt of quarterly Information Governance reports. The IGWG will monitor operational progress throughout the year and take action to address any concerns, and deficiencies will be noted and reviewed at subsequent meetings.

- **Statistically validated reduction in Information Governance related incidents.**
  Monthly monitoring of incidents by the Caldicott Guardian and quarterly through the IGWG.

- **No Data Protection Act monetary penalties, enforcement notices, or undertakings served on the Trust. No Freedom of Information Act enforcement notices served on the Trust.**
  The Trust Board and Quality Committee will monitor progress through receipt of quarterly Information Governance reports.

- **Staff know who and where to direct information governance concerns and queries to.**

8.0 Legislation and Guidance

8.1 Data Protection Act 2018
General Data Protection Regulation (GDPR) 2016
Freedom of Information Act 2000
Environmental Information Regulations 2004
Human Rights Act 1998
Common Law Duty of Confidentiality
Protections of Freedoms Act 2012
ISO 15489 Records Management
ISO 27001 Information Security Management

9.0 Appendices

Appendix A: Definitions

Personal Data	Personal Data is any information relating to natural persons: • who can be identified or who are identifiable, directly from the information in question; or • who can be indirectly identified from that information in combination with other information.
Special Categories of Data	Special Categories of Data is any personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, or data concerning a person’s sex life or sexual orientation.
Data Controller	The entity that, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data Processor	An entity that processes data on behalf of, and only on the instructions of, the relevant Data Controller.
Data Subject	Any natural person whose personal data is processed by a controller or processor.
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Third Party	Any individual/organisation other than the data subject, the data controller (the Trust) or its agents.
Consent	Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
Healthcare Purposes	Includes all activities that directly contribute to the diagnosis, care and treatment of an individual and the audit/assurance of the quality of the healthcare provided. Does not include research, teaching, financial audit and other management activities.
Anonymised Data	Information which does not relate to an identified or identifiable natural person.

Pseudonymisation	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Appendix B: Roles & Responsibilities

Chief Executive

As the accountable officer for the Trust, the Chief Executive has overall responsibility for compliance with the GDPR and Data Protection Act 2018. Operational responsibility for data protection is delegated to the Senior Information Risk Owner (SIRO), Data Protection Officer and all Information Asset Owners (IAOs).

Senior Information Risk Owner (SIRO)

The Board-level SIRO, under delegated authority from the Chief Executive, oversees compliance with the Data Protection Act and is responsible for the Trust's information risk. The Trust's SIRO is the Executive Director of Quality, Governance and Performance Assurance. The SIRO is supported by the Data Protection Officer, Information Asset Owners, and Information Governance Team.

Caldicott Guardian

The Caldicott Guardian is responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing. The Caldicott Guardian is responsible for providing advice within the Trust on the lawful and ethical processing of patient information. The Executive Medical Director acts as the Trust's Caldicott Guardian and is supported on a day to day basis by the Deputy Medical Director who plays a key role in ensuring that the organisation satisfies the highest practicable standards for handling patient identifiable information.

Data Protection Officer (DPO)

A Data Protection Officer (DPO) is a role mandated for public bodies, for organisations carrying out regular and systematic monitoring of data subjects on a large scale, and for organisations carrying out large scale processing of special category data (e.g. health and social care) or criminal convictions data. The Head of Corporate Affairs acts as the Trust's DPO and is supported on a day to day basis by the Information Governance Team. The DPO advises the organisation on data protection matters, monitors compliance and is a point of contact on data protection for the public and the ICO.

Associate Director of Performance Assurance and Risk

The Associate Director of Performance Assurance and Risk on behalf of the Trust Board is responsible for the ongoing delivery of this policy/framework. He/she will provide regular reports to the Quality Committee on progress against its implementation.

Quality Committee
This policy/framework will be overseen by the Quality Committee, chaired by a Non-Executive Director of the Trust. This committee will received assurance of ongoing progress against the policy/framework.

Trust Management Group
The Trust Management Group, chaired by the Chief Executive, will receive policies and proposals for approval.

Information Governance Team
The Information Governance Team provides day-day-day operational support to the SIRO and Caldicott Guardian and is responsible for providing general advice and guidance on data protection and the application of this policy.

Information Asset Owners (IAOs)
The SIRO is supported by a network of Information Asset Owners (IAOs) and Information Asset Administrators (IAAs). These individuals are responsible for interpreting information governance policy, applying it on a practical level within their area of responsibility and ensuring that policies and procedures are followed by staff. They recognise actual or potential security incidents, consult with the SIRO and Caldicott Guardian in relation to incident management and ensure that ROPA are accurate and up to date.

Information Governance Working Group (IGWG)
The Information Governance Working Group (IGWG) consists of all Information Asset Owners (IAOs).

All Staff
All staff are responsible for making sure they have read and understood this policy and associated procedures and are aware of the disciplinary and legal action that could potentially be taken if this policy and associated procedures are not followed. Compliance with data protection legislation is the responsibility of all members of staff including anyone providing a service on behalf of the Trust.