Medway NHS Foundation Trust
Corporate Policy: Information Governance and Framework

Author:	Anne Bailey Information Governance Manager
Document Owner	Alison Davis – Chief Medical Officer
Revision No:	6
Document ID Number	POLCGR129
Approved By:	Information Governance and Policy Compliance Group and Policy Compliance Group
Implementation Date:	September 2022
Date of Next Review:	September 2024

Medway NHS Foundation Trust
Information Governance Policy

Document Control / History	
Revision No	**Reason for change**
1	New document combined Information Governance Framework, Policy and Strategy
2	Annual review 2017
3	Annual review 2018, inclusion of GDPR, revision from IG toolkit to DSP toolkit
4	Annual review 2019, removal of IG Strategy, and change of owners, inclusion of well lead CQC requirements
5	Review and update SIRO from Director of IT to Deputy Chief Executive
5.1	Training Needs Analysis added
6	Update SIRO

Consultation
SIRO
Information Governance Committee
Head of Corporate Governance & Legal

Medway NHS Foundation Trust
Information Governance Policy

Table of Contents

Medway NHS Foundation Trust
Information Governance Policy

To be read in conjunction with any policies listed in Trust Associated Documents.

1 Introduction

1.1 Information Governance (IG) is, at its simplest, a framework that draws together statutory, mandatory and best practice standards about the management of information - whether personal (patient or staff) or corporate. Good quality information is at the heart of decisions made by staff, not only in terms of patient care but also in the management of the organisation and maintaining public confidence in the services that the Trust provides.

1.2 The Trust is required to evidence its compliance with these standards through the Data Security & Protection (DSPT), which sets a route map for self-assessment and improvement against set criteria year on year in addition to performance against data security.

2 Purpose / Aim and Objective

2.1 **Information Governance Framework and Policy Statement**

Medway NHS Foundation Trust has defined governance structures laid out in the IG framework. These set the governance, accountability and responsibilities for ensuring it maintains and improves standards of IG compliance aligned to an Information Governance Strategy that evidentially supports the DSPT requirements.

2.2 The Policy framework ensures that key compliance areas provide the Senior Information Risk Owner (SIRO) with timely, reliable and fit for purpose information to meet reporting requirements, to support legislative and regulatory compliance and to assist in management decision making. Trust managers will provide commitment and leadership in respect of IG and ensuring information is accurate, robust and timely.

2.3 Assurances will be provided to the Trust Board through reports from the Information Governance team and DPO (Data Protection Officer) - these reports will promote openness and transparency in how the Trust is progressing against the DSPT requirements, and highlight key areas of risk and non-compliance.

2.4 The Trust aims to 'Be the BEST' in everything it sets out to, and this extends to embedding IG at the heart of how it protects, manages and uses patient, staff and corporate information.

2.5 Ensure that we are able to evidence to the CQC that the Trust is well led in Information governance and we can evidence that we meet best practise principles in relation to::

- Availability: Data must be available when and where it is needed. It must be made accessible swiftly and securely for staff as well as within and between organisations

- Integrity: The data must be valid and trustworthy, relevant, up to date, and protected from loss, damage, and unauthorised alteration.
- Confidentiality: Personal identifiable data must be handled and used

3 Policy Framework

3.1 **Medway NHS Foundation Trust** is committed to complying with statutory, mandatory and best practice requirements through a supporting framework of documents:

Information Security Policy POLCGR018 - Information Security Policy The Trust's Information Security policy is a high level document that utilises a number of controls to protect the organisation's information. The controls are delivered through policies, standards, processes, procedures, supported by tools and user training.
USB, Removable Media and Media Destruction Policy POLCGR086 - USB, Removable media and Media Destruction Policy This policy supports the Information Security Policy to ensure that strict procedures are followed to prevent patient and staff personal data is not compromised, lost or stolen through the use of removable media.
Records Management & Lifecycle Policy STRCGR002 - Records Management & Lifecycle Policy The Trust's records are its corporate memory, providing, evidence of actions and decisions, and representing a vital asset to support daily functions and operations. Records support policy formation and managerial decision-making, protect the interests of the Trust and the rights of patients, staff and members of the public. They support consistency, continuity, efficiency and productivity and help deliver services in consistent and equitable ways. This document governs the cycle of records from their collection to disposal.
Data Protection Policy POLCGR007 - Data Protection Policy This policy provides a framework for the Trust to ensure compliance with its confidentiality obligations, and in particular the General Data Protection Regulation (GDPR) and the Data Protection 2018. The Trust, as a Data Controller, has a legal obligation to comply with all appropriate legislation with regard to the processing of personal data. It also should comply with guidance issued by the Department of Health, NHS England, other advisory groups to the NHS, and guidance issued by professional bodies.

This includes the Trusts responsibilities for completing Data Privacy Impact assessments when we are using new systems or using patients or staff information in a different way SOP0363-Conducting a DPIA
Freedom of Information Policy POLCGR009 - Freedom of Information Act 2000 Policy This policy provides a framework for the Trust to ensure compliance with the FOIA, Re-use of Public Sector Information Regulations 2015 and the Environmental Information Regulations 2004.
Use of Cameras, video and audio recorders on Trust premises GUCGR023 - Use of cameras video and audio recorders on Trust premises Policy and Procedure This guidance ensures that patient images remain confidential and for the purposes of helping with the assessment and evaluation of a patient's condition through the use of clinical photography; and service users and patients do not make recordings (covert or otherwise) of other patients, or staff engaged in clinical interventions with patients.
Secure Transfer of Information Policy POLCGR077 - Secure Transfer of Information Policy This policy governs the transfer of patient identifiable or staff identifiable information. Its aim is to ensure such transfers meet Caldicott principles in preventing information becoming lost in transit, erroneously sent to the wrong person or sent to the correct destination but in an insecure manner.
Acceptable Use of Trust Information Systems and Assets POLCGR113 - Acceptable Use of Trust Information Systems and Asset Policy The aim of this policy is to ensure the proper use of the Trust's NHS information systems and assets and make users aware of what the Trust deems to be acceptable and unacceptable use of these.
Data Assurance Policy POLCOM037 - Data Quality Policy This policy describes why Data Quality and assurance is important to the Trust; where responsibilities for maintaining and improving Data Quality lie; the means by which its continual improvement will be effected; and the processes which will ensure that the Board can be assured over the effectiveness of the systems, processes and controls over reported performance information.
Network Security Policy POLCGR082 - Network Security Policy This policy sets out the goals of protecting systems from misuse and keeping them available to users. It aims to ensure the confidentiality, integrity and availability of the Trust's information assets.
Registration Authority (RA) Policy POLCGR093 - Registration Authority

This policy applies to all processes, procedures and activities carried out by the RA in relation to Trust systems which require Smartcard

4 Roles and Responsibilities

4.1 Trust Board

4.1.1 The Trust Board is ultimately responsible for ensuring that the Trust corporately meets its legal responsibilities and for the adoption of internal and external governance requirements.

4.1.2 The Trust Board is responsible for approving the Trust's Corporate Policy for information governance.

4.1.3 The Trust Board is responsible for reviewing reports from the SIRO, Data Protection Officer (DPO) and Caldicott Guardian to the Board on information governance arrangements.

4.1.4 The Trust Board is responsible for understanding the statutory framework and assuring itself on the adequacy of the Trust arrangements for meeting requirements.

4.2 Chief Executive

4.2.1 The Chief Executive has overall responsibility for ensuring that sufficient resources are provided to support information governance requirements.

4.3 Caldicott Guardian

4.3.1 The Chief Medical Officer is the Trust's Caldicott Guardian who is responsible for ensuring that MFT satisfies the highest practical standards for handling patient identifiable information. The role encompasses:

- acting as the 'conscience' of MFT;
- facilitating and enabling information sharing and advising on options for lawful and ethical processing of information;
- representing and championing Information Governance requirements and issues at Board level;
- receiving training as necessary to ensure they remain effective in their role as the Caldicott Guardian;
- ensuring that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff; and

- overseeing all arrangements, protocols and procedures where confidential patient information may be shared with external bodies both within, and outside, the NHS.
- Is the Chair of the Information Governance Group, ensuring upward reporting to the Risk and Compliance Assurance Group;

4.4 **Senior Information Risk owner (SIRO) - Currently Director of IT**

4.4.1 is the designated Executive Lead for Information Governance with responsibility for ensuring that the Trust has plans and policies in place to fulfil the requirements of the statutory framework;

4.4.2 acts as champion for information risk on the Board and provides written advice to the Accounting Officer on the content of the Organisation's Annual Governance Statement in regard to information risk;

4.4.3 understands how the strategic business goals of MFT and how other NHS organisations' business goals may be impacted by information risks, and how those risks may be managed;

4.4.4 implements and leads the NHS Information Governance risk assessment and management processes within MFT;

4.4.5 advises the Board on the effectiveness of information risk management across MFT; and

4.4.6 Is the Trust Senior Information Risk Owner (SIRO) with responsibility for fulfilling the requirements of the role.

4.5 **Director of IT**

The formulation and implementation of ICT related policies and the creation of supporting procedures, and ensuring these are embedded within the service developing, implementing and managing robust ICT security arrangements in line with best industry practice;

4.5.1 Effective management and security of Trust

- resources, for example, infrastructure and equipment;
- Developing and implementing a robust IT Disaster Recovery Plan;
- Ensuring that ICT security levels required by NHS Statement of Compliance are met;
    - Ensuring the maintenance of all firewalls and secure access servers are in place at all times, and;
    - Ensuring the provision of Information Asset Owners for the ICT infrastructure with specific accountability for computer and telephone equipment and services that are operated by corporate and clinical work force, e.g. personal computers,

laptops, personal digital assistants and related computing devices, held as a NHS asset.

4.6 **Divisional Director of Operations for Care Groups (Planned and Unplanned)**

4.6.1 The Divisional Director of Operations (Planned Care) is responsible for the management and delivery of the function of health records management in accordance with information governance policies.

4.6.2 Ensure staff within their areas are following Trust policies and guidance and are operating there services in a safe and effective way when it comes to Information Governance.

4.7 **Information Governance Group**

4.7.1 This Group is established on the authority of the Risk and Compliance Assurance Group to assist the Trust Board in fulfilling its responsibilities in relation to information governance. Its purpose is to monitor and co-ordinate implementation of the Information Governance Policy and the DSPT - requirements and other information related legal obligations. Terms of Reference setting out the full responsibilities of the Group are available here.

4.8 **Information Asset Owners (IAO), who will:**

4.8.1 lead and foster a culture that values, protects and uses information for the success of MFT;

4.8.2 know what information comprises or is associated with the asset, and understands the nature and justification of information flows to and from the asset;

4.8.3 receive training as necessary to ensure they remain effective in their role as an Information Asset Owner;

4.8.4 know who has access to the asset, whether system or information, and why, and ensures access is monitored and compliant with policy; and

4.8.5 understand and address risks to the asset, and provide assurance to the SIRO.

4.9 **The Information Governance Manager, who will:**

4.9.1 maintain an awareness of Information Governance issues within MFT

4.9.2 act as the operational lead for delivery of the Information Governance agenda;

4.9.3 Manage the information governance team;

4.9.4 review and update the suite of Information Governance policies, strategies, framework and guidance in line with local and national requirements;

- review and audit all procedures relating to this policy where appropriate on an ad-hoc basis; and
- ensure that staff are aware of the requirements of the policy.
- Providing expert advice and guidance to all staff on all elements of Information Governance.
- Developing internal Information Governance policies and procedures to meet NHS information governance guidance and legislation.
- Developing Information Governance awareness and training programmes for staff.
- Ensuring compliance with Data Protection, Information Security and other information related legislation.
- Co-ordinating the response to freedom of information requests.

4.10 **Line Managers**

4.10.1 Line managers are responsible for ensuring that the Information Governance Policy is implemented within their group or directorate.

4.11 **All Staff**

4.11.1 All staff are responsible for adhering to the policy and fulfilling mandatory training requirements.

5 Monitoring and Review

What will be monitored	How/Method / Frequency	Lead	Reporting to	Deficiencies/ gaps Recommendations and actions
Policy review	Annually	Information Governance Manager	SIRO & IG Group	Where gaps are recognised action plans will be put into place
Compliance with the Trust's DSPT requirements	Managed via (1) quarterly feedback to the IG Group (2) Half year SIRO reports to Board	(1) IG Manager (2) Head of Integrated Governance and Legal	(1) The IG Group (2) The Executive Group	Where gaps are recognised action plans will be put into place

6 Training and Implementation

6.1 In order to meet the statutory requirement on the Trust for data protection training and regulatory requirements around IG and data security, it is necessary for the Trust to ensure that all staff are aware of and understand what is expected of them in this respect when carrying out duties.

6.2 The key messages that need disseminating under this strategy are:

6.2.1 Mandatory IG messages

6.2.2 Targeted IG messages around IG related areas

6.2.3 Key messages arising from IG risks/incidents (both serious and common)

6.2.4 Role specific training.

6.3 The training needs analysis can be found in appendix 1.

6.4 The staff identified have a particular focus and responsibility around IG and it is important that they are well informed across all aspects of IG.

6.5 The training required by these staff is not necessarily required annually, but in order to keep current should be repeated on a periodic basis, for example a cycle of every three years.

6.6 In addition IG specialist staff (such as FOI's, SARs, DPO, IG Manager, Information Security Manager etc) are required to undertake specialist training in their area of responsibility in order to maintain their expertise and currency. This is also a DSPT requirement and a requirement under the Data Protection Principle of *Integrity and confidentiality (security).*

6.7 To support the staff complete their mandatory training, e-learning training is available also supported by face to face sessions and bespoke training for dedicated cohorts and staff groups e.g. estates and facilities staff groups and staff who work out of hours are arranged twice year.

7 Equality Impact Assessment Statement & Tool

7.1 All public bodies have a statutory duty under the Race Relation (Amendment) Act 2000 to "set out arrangements to assess and consult on how their policies and functions impact on race equality." This obligation has been increased to include equality and human rights with regard to disability, age and gender.

7.2 The Trust 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. This document was found to be compliant with this philosophy.

7.3 Equality Impact Assessments will also ensure discrimination does not occur on the grounds of Religion/Belief or Sexual Orientation in line with the protected characteristics covered by the existing public duties.

9 References

Document	Ref No
References:	
NHS Digital Data Security & Protection toolkit	
General Data Protection Regulation (GDPR) and the Data Protection 2018	
Freedom of Information Act 2000	
Information Security Management ISO 27001	
Information Governance Alliance Code of Practice on Records Management	
NHS Confidentiality Code of Practice	
Trust Associated Documents:	
POLCGR079 - User Access Management Policy	POLCGR079
SOP0247 - Subject Access Requests and Access to Health Records Procedure	SOP0247
OTCGR139 - Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation	OTCGR139
OTCGR004 - Code of Conduct For Staff in Respect of Confidentiality	OTCGR004
OTCGR040 - Kent and Medway Information Sharing Agreement	OTCGR040

Appendix 1 – Training Needs Analysis

Staff Group	Training Type	Frequency
All staff	**Data security awareness / IG training**	Before starting with Trust and annually thereafter Mandatory
	Risk basis training will be provided by IG where the need is identified through • Analysis of AI reports, areas identified as having high volume of IG related incidents • Serious IG incident or serious IG miss • Analysis of responses to awareness surveys	As and when required
PID staff **System Managers** **IT Project Managers** **Service Improvement managers** **R & I staff** **Researchers**	**Sharing Confidential Information** Training for staff working with PID for analysis, provision of reports and sharing information external to the Trust. Researchers whose research involves PID being shared or processed externally.	At least once Mandatory
All IG related roles • **SIRO** • **Caldicott guardian** • **Head of IG / Data Protection Officer** • **IG manager** • **Records Managers** • **Registration Authority Managers** • **SARs and FOI Team** • **Project Managers** • **Service Managers**	**IG training** All staff working in IG related roles need to ensure that they are suitably trained and/or qualified to undertake their roles and are up to date on the latest legislation, regulations and developments in their respective areas. There is no longer nationally provided role-specific training, therefore this training must be either provided in-house or out-sourced depending on the subject and number of staff involved.	At least once Mandatory

Staff Group	Training Type	Frequency
Data Quality staff	**Data Quality Training** For staff capturing and/or entering data (particularly patient data) within the Trust. Includes legal requirements for data accuracy, information on the False or Misleading Information Regulations and impact of poor data quality, including potential breaches of confidentiality.	Once a year Mandatory
Legal Team – FOI and SAR's **HR Team** **Governance Team** **Quality Team**	**Redaction and Scrutiny Training** All staff involved in the release of confidential information or at the very least one team member of each team involved in releasing confidential or sensitive information has taken redaction and scrutiny training. Includes staff who provide information in response to other requests for personal or sensitive / confidential information	At least once Mandatory

END OF DOCUMENT