Wirral Community Health and Care NHS Foundation Trust

Information Governance Policy
IG01
Version 5

TRUST-WIDE NON-CLINICAL

Document detail	
Policy Number	IG01
Version	Version 5
Approved by	Finance and Performance Committee
Effective from	October 2021
Date of last review	08/2024
Date of next review	08/2027
Lead Director	Director of Corporate Affairs (SIRO)
Responsible Lead	Information Governance Manager / Data Protection Officer
Superseded documents	IG01 Information Governance Policy, IG04 Caldicott and Data Protection Policy, IG01 Information Governance and Data Protection Policy
Document summary	This Policy establishes Wirral Community Health and Care NHS Foundation Trust information governance framework, sets out the high-level information governance principles required to ensure compliance with legislation, effective management and protection of organisational and personal information and sets out responsibilities and reporting lines for staff.

Document History		
Version number	Comments	Approved by
	This policy merges and updates the IG01 Information Governance Policy and IG04 Caldicott and Data Protection Policy.	Quality and Safety Committee
3	This policy has been updated to ensure that it provides a clear statement of organisational intent in relation to information governance. This has led to the policy being separated into an Information Governance and Data Protection Policy.	
4	Following the review of the committee terms of reference in October 2023, the role of the finance and performance committee to receive assurance on information governance compliance have been strengthened. The finance & performance committee now review and approve the information governance policies (including this Policy) which were previously approved by the Quality & Safety Committee.	Quality & Safety Committee and Finance & Performance Committee
5	Review required as policy last reviewed 3 years ago.	Finance and Performance Committee

Policy on a Page

This policy establishes the Trust's information governance framework, sets out high level information governance principles required to ensure compliance with legislation, effective management, and protection of organisational and personal information, and sets out responsibilities and reporting lines for staff.

Key Information Governance roles within the Trust include the Senior Information Risk Owner, Caldicott Guardian, Chief Digital Information Officer, Information Governance Lead, and the Data Protection Officer.

This policy applies to all employees of the Trust, including Non-Executive Directors, Governors, bank staff, volunteers, individuals on secondment and trainees or those on a training placement within the Trust as well as locum or temporary staff employed through an agency.

The five strands of the Trust's Information Governance Policy are:

- Transparency
- Legal and Regulatory Compliance
- Information and Cyber Security
- Information Quality Assurance and Management
- National Data Security Standards

The policy outlines how the Trust and staff will meet each strand to ensure high standards of Information Governance practice.

It is compulsory for all new starters to complete onboarding prior to commencement in their post. Onboarding provides new employees with a data protection and security induction.

Managers must complete a local induction checklist with new starters. The local induction checklist requires managers to inform staff about the importance of information governance, information governance training requirements and to provide copies of the Information Governance Policy and Policy for Confidentiality Code of Conduct.

Staff are required to complete the Trust's information governance training annually (e-Learning for Healthcare Data Security Awareness Level 1) through ESR.

Staff should be aware that failure to comply with this policy, associated policies, and procedures and/or their Information governance responsibilities is serious and could result in a number of sanctions including:

- Disciplinary action up to and including dismissal.
- Criminal charges
- Investigation and potential removal of registration by relevant Professional Body i.e. Nursing and Midwifery Council

CONTENTS **Page No.**

1. PURPOSE AND RATIONALE

Information is a vital asset to Wirral Community Health and Care NHS Foundation Trust (the Trust) both in terms of the management of patients and service users and the efficient management of services and resources. Information is a fundamental aspect of clinical and corporate governance, service planning and performance management.

This policy establishes the Trust's information governance framework, sets out high level information governance principles required to ensure compliance with legislation, effective management, and protection of organisational and personal information, and sets out responsibilities and reporting lines for staff.

This policy and its associated policies and procedures ensure that information processed by the Trust is protected from breaches of confidentiality, integrity, and availability.

Staff should be aware that failure to comply with this policy, associated policies, and procedures and/or their Information governance responsibilities is serious and could result in a number of sanctions including:

- Disciplinary action up to and including dismissal.
- Criminal charges
- Investigation and potential removal of registration by relevant Professional Body i.e. Nursing and Midwifery Council

2. OUTCOME FOCUSED AIMS AND OBJECTIVES

The objectives of the Information Governance Policy are to establish:

- the Trusts position on information governance
- a foundation on which actions, processes, associated policies, and procedures will be based.
- the mandate for the scope of information governance activities
- key actions with assigned responsibilities
- a requirement for all staff to adhere to the policy.

3. SCOPE

This policy applies to all:

- employees of the Trust, including Non-Executive Directors, Governors, bank staff, volunteers, individuals on secondment, trainees, those on a training placement as well as locum or temporary staff employed through an agency.
- areas of Trust business, for example, clinical divisions, finance, HR, estates
- information created and received.
- formats of information for example, clinical/care records, emails, voice messages, minutes, text messages, instant messages, photographs, staff records, financial records, and facilities records
- information systems and applications
- equipment used to process information for example, laptops, computers, mobile phones, cameras.
- social media, for example Linkedin

4. RESPONSIBILITIES, ACCOUNTABILITIES AND DUTIES

Chief Executive Officer
The Chief Executive has overall accountability and responsibility for information governance in the Trust.

Trust Board
The Board will review information governance concerns escalated from the Information Governance and Data Security Group via the Finance & Performance Committee.

Senior Information Risk Owner
The Trust's Senior Information Risk Owner (SIRO) has executive responsibility for the management and mitigation of all information risk.

The SIRO will:

- review and agree action in respect of identified information risks.
- brief the Board on identified information risk issues.
- ensure that all information assets have assigned information asset owners.
- annually sign off the information asset register
- ensure that the organisation's approach to information risk is effective in terms of resource, commitment, and execution and that it is communicated to staff.
- take ownership of the risk assessment processes for information and cyber risk.
- sign off the annual Data Security and Protection Toolkit prior to submission.
- oversee the development and implementation of an incident risk policy*
  (NHS Digital, 2018)

*the Trust has in place the Policy for Risk Identification and Management and the Incident Management Policy, both available on Staff Zone.

The SIRO is a core member of the Information Governance and Data Security Group and reports directly to the Chief Executive Officer. The SIRO is Lead Director for this policy.

Caldicott Guardian
The Trust's Caldicott Guardian has a strategic role with regard to representing and championing information governance and confidentiality at Board and, where appropriate throughout the Trust.

The Caldicott Guardian will:

- ensure that personal information collected about patients / service users is used legally, ethically, and appropriately, and that confidentiality is maintained.
- apply the eight Caldicott Principles wisely, using common sense and an understanding of the law.
- actively support work to enable information sharing where it is appropriate to share and advising on options for lawful and ethical processing
  (UK Caldicott Guardian Office, 2017)

The Caldicott Guardian is a core member of the Information Governance and Data Security Group and reports directly to the Chief Executive Officer.

Finance and Performance Committee

The Finance and Performance Committee (FPC) is the responsible committee for the final approval of this policy.

The FPC will:

- receive assurance that the Trust meets its statutory and regulatory obligations in relation to information governance via the Information Governance and Data Security Group
- review concerns escalated to them, action those relevant to the Committee's terms of reference and refer, as appropriate, to the Board.
- encourage and review incident reporting within the Trust.

Information Governance and Data Security Group

The Trust's Information Governance and Data Security Group is responsible for reviewing and approving this policy prior to ratification by QSC.

The Information Governance and Data Security Group will:

- monitor Freedom of Information and Subject Access Request compliance
- receive Cyber Security assurance through monthly IT Security Group report and Cyber Security (patching, AV alerts and careCERTs) update.
- provide operational Information Governance and Data Security guidance and support to staff.
- have oversight and monitoring responsibilities of the annual Data Security and Protection Toolkit submission.
- develop and review policies, SOPs and guidance associated with Information Governance and Digital, Data Security and Protection Toolkit action plans, and Caldicott associated issues.
- monitor mitigations, controls and progress of Information Governance and Data Security risks.
- review and approve Data Protection Impact Assessments as part of a privacy by design approach.
- monitor Information Governance / Record Keeping incidents and trends, system access audits outcomes, SAFE IG checklist compliance and data quality metrics and reports.
- promote and increase awareness of cyber security and information governance issues to the Finance & Performance Committee, Board of Directors, and staff.
- oversee and monitor completion of the Information Asset Register and System Level Security Policies
- monitor staff compliance with annual Data Security Awareness training and review training needs analysis of staff with specialist roles in data protection and securityR

Information Governance Lead

The Information Governance Lead is the author of this policy.

The Information Governance Lead will:

- manage and oversee the Trust's information governance agenda.
- provide specialist information governance advice and guidance to staff.
- monitor compliance with information governance policies and procedures and ensure policies are in line with legislative and regulatory requirements.
- maintain an awareness of information governance issues within the Trust.
- submit an annual information governance report to the Board.
- complete SBAR and RCA investigations as and when required and subsequently support the development of actions plans.
- report information governance risks on the risk register and to the SIRO.

- ensure compliance with and annually submit the DSPT.
- support the teams that handle subject access requests and Freedom of Information requests.
- assess information governance incidents and when required onward report to Information Commissioner's Office (ICO) and/or Department of Health
- provide support and advice to Information Asset Owners in relation to their assets.
- develop and deliver bespoke information governance training.
- be a core member of the Information Governance and Data Security Group
- provide support and work closely with the SIRO and Caldicott Guardian on information governance issues.

Data Protection Officer

The DPO will:

- monitor organisational compliance with data protection legislation.
- inform and advise on data protection obligations.
- review Data Protection Impact Assessments (DPIAs)
- cooperate with the ICO.
- be the first point of contact for the ICO and individuals whose data is processed by the Trust (patients, service users, staff, volunteers etc.)
  (NHS Digital 2018)

Chief Digital Information Officer

Chief Digital Information Officer will:

- develop, implement, and enforce suitable and relevant information security policies and procedures to ensure the Trust's systems and infrastructure remain in line with best industry practice and compliant with data protection legislation.
- ensure electronic equipment and assets have adequate security measures to comply with data protection and data security legislation and regulations.
- develop and implement a robust IT Disaster Recovery Plan
- monitor and review reported information and cyber security incidents through the incident reporting system.
- report information and cyber security risks on the risk register and inform the SIRO.
- support and advise Information Asset Owners in relation to their information assets.
- evidence compliance with allocated DSPT assertions
- to be a core member of the Information Governance and Data Security Group
- work with the Information Governance Manager and DPO as appropriate regarding matters relating to data and IT security

Information Asset Owners

Information Asset Owners (IAOs) will:

- promote a culture that values, protects, and uses information for the benefit of patients, service users and staff.
- understand the flows of information to and from the information asset(s)
- monitor and review who has access to information asset(s), ensure access is legitimate and audit access to information within the asset.
- assess risk to the information asset and provide assurance to the SIRO via the Information Governance and Data Security Group
- ensure there is a legal basis for the processing of personal data.
- seek advice in relation to the above from the Information Governance Manager and/or Chief Digital Information Officer
- ensure information assets are recorded, monitored, and updated on the Information Asset Register
- attend the quarterly Information Asset Owner/Administrator meeting and comply with the annual action plan.

- undertake specialist information asset training as and when required

Divisional/Locality Managers and Service Leads
Divisional/Locality Managers and Service Leads will:

- ensure the Information Governance Policy is implemented within their divisions and ensure service level procedures are compliant with the Information Governance Policy
- take ownership of, and seek to improve, the quality of information within their services.
- monitor staff compliance with e-Learning for healthcare Data Security Awareness Level 1
- encourage staff to report any information governance and data security incidents via the incident reporting system immediately.
- report any identified information risks relating to their divisions/services on the Trust's risk register.

All Staff
This policy applies to all employees of the Trust, including Non-Executive Directors, Governors, bank staff, volunteers, individuals on secondment and trainees or those on a training placement within the Trust as well as locum or temporary staff employed through an agency.

Staff will:

- ensure that they adhere to this policy and all associated information governance and data security policies and procedures.
- complete annual information governance training (e-Learning for Healthcare Data Security Awareness Level 1) via the Electronic Staff Record (ESR)
- report identified information governance incidents on the Trusts incident reporting system.

5. PROCESS

The eight Generally Accepted Recordkeeping Principles (GARP) (ARMA International, 2017) have been used to assist the development of the Trust's information governance framework.

The eight GARP principles are:

- Accountability
- Transparency
- Integrity
- Protection
- Compliance
- Availability
- Retention
- Disposition

The eight principles have been captured within the five areas listed below.

The five strands of the Trust's Information Governance Policy are:

- Transparency
- Legal and Regulatory Compliance
- Information and Cyber Security
- Information Quality Assurance and Management
- Cyber Assurance Framework

Transparency

The Trust will register as a data controller that is processing personal information with the ICO.

The Trust will ensure information governance policies and procedures are available to staff via Staff Zone and will inform staff of any new or updated policies via the Staff Bulletin.

The Trust will maintain an up-to-date Information Asset Register that encompasses data flows in and out of assets.

The Trust will provide data subjects with a privacy notice that informs them of who the Trust are, contact details for the Trust's Data Protection Officer, the purpose for which personal data is collected and used, how the data is used and disclosed, how long it is kept, and the legal basis for processing.

The Trust will support data subjects to exercise their right to access information processed about them.

The Trust will ensure compliance with the requirements of the Freedom of Information (FOI) Act 2000 through the development, maintenance, and communication of an FOI policy.

Non-confidential information about the Trust and its services will be available to the public through a variety of media communications.

The Trust's Communication Team will establish clear procedures for communicating with the media.

Where the Trust uses CCTV systems it will ensure that appropriate signage is visible to individuals prior to them entering a surveillance area.

In the event of a data breach that results in a risk to the rights and freedoms of an individual the Trust will inform the affected individual of the incident.

Legal and Regulatory Compliance

The Trust will ensure that it's information governance framework and associated policies and procedures meet the legislative and regulatory requirements. These include but are not restricted to the following:

- Data Protection Act 2018
- UK General Data Protection Regulations
- Health & Social Care (Quality & Safety) Act 2015
- Common Law Duty of Confidentiality
- The Privacy and Electronic Communications Regulations 2003
- Health & Social Care Act 2012
- National Health Service Act 1977, 2006
- Freedom of Information Act 2000
- Public Records Act 1958, 1967 and 2005
- Network & Information Systems Regulations 2018
- Information: To Share or Not to Share? The Information Governance Review (National Data Guardian, 2003)
- The Eight Caldicott Principles (National Data Guardian, 2020)
- Confidentiality: NHS Code of Practice (Department of Health and Social Care, 2003)

- Records Management Code of Practice 2021 (NHSX, 2021)
- Data Security & Protection Toolkit based on the Cyber Assurance Framework (CAF)
- National Data Guardian for Health and Care Review of Data Security, Consent and Opt-Outs (National Data Guardian, 2016)
- Care Quality Commission Standards
- Environmental Information Regulations 2004
- Human Rights Act 1998
- Access to Health Records Act 1990
- Serious Crime Act 2015
- Electronic Communications Act 2000
- Public Interest Disclosure Act 1998
- The Procurement Regulations 2024

Information and Cyber Security

The Trust will ensure an appropriate level of protection and security to information that is personal, confidential, privileged, secret, classified, essential to business continuity, or that otherwise requires protection.

All information assets will be captured on the Trust's information asset register, have allocated Information Asset Owners and the data flows in and out of each asset will be risk assessed.

The Trust will ensure compliance with the Cyber Essentials Plus standard or equivalent.

The Trust will conduct or commission annual assessments and audits of its information and cyber security arrangements.

Staff will be provided with clear guidance on keeping personal information and commercially sensitive information secure, sharing information safely and lawfully and on respecting the confidentiality of patients and service users.

The Trust will grant staff appropriate and role relevant levels of access to confidential information and access will be audited to ensure access to records is legitimate.

A data protection by design and default approach will be embedded within the organisation in line with the Data Protection by Default and Design Standard Operating Procedure.

The Trust will complete Data Protection Impact Assessments (DPIA) when proposed processing is likely to result in a 'high risk' to the privacy of individuals.

The Trust will ensure services have developed Business Continuity Plans in line with the Emergency Planning, Resilience and Response Policy.

The Trust will maintain the Incident Management Reporting Policy and the Standard Operating Procedure for Personal Data Breaches and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.

The Trust will maintain its Risk Register in line with its Policy for Risk Identification and Management.

Information Quality Assurance and Management

The Trust will maintain information in a manner that ensures timely, efficient, and accurate retrieval.

Electronic information will be backed up to ensure that it can be restored if there is a disaster, system malfunction or if data becomes corrupt.

Staff will be encouraged to complete annual data cleanses to remove obsolete and jobless information as per the Records Management Policy.

The Trust will aim to ensure the integrity and authenticity of records through the provision of record keeping training for staff, the use of audit trails and by maintaining the reliability of systems used to record information.

The Trust will develop, maintain, and communicate policies and procedures for information quality assurance and effective and efficient records management to ensure information is accurate, available, reliable, and recorded contemporaneously.

The Trust will annually audit information quality and records management against standards set out in both the Records Management Policy.

The Trust will retain information in line with the records retention schedule outlined within 2021 NHS England's Records Management Code of Practice 2023.

The Trust will ensure secure and appropriate disposition of information that reaches the end of its retention.

National Data Security Standards

The Trust will adopt the National Cyber Security Centre's Cyber Assessment Framework (CAF) as its basis for cyber security and IG assurance from September 2024.

The Trust will provide assurance of compliance with the CAF and meeting their legislative obligations on data protection and data security through annual submission of the Data Security and Protection Toolkit (DSPT.) The Trust's annual submission will be audited by internal audit.

The CAF structure consists of 39 outcomes, grouped into four objectives and a number of principles**.**

The four objectives are:

Objective A
Managing risk

Objective B
Protecting against cyber-attack and data breaches

Objective C
Detecting cyber security events

Objective D

Minimising the impact of incidents

Each outcome is supported by indicators of good practice, representing characteristics likely to be found in organisations meeting the outcome at any of three levels – Not Achieved, Partially Achieved or Achieved.

The most important element of the CAF is the outcome as some indicators may not apply in particular situations, and there may be different ways to meet the outcomes (particularly for the more technical security outcomes). Expectations on organisations are therefore set at the outcome level.

6. RELATED POLICIES

This policy underpins the following policies/procedures:

Policy Name
Data Protection and Confidentiality Policy
Individual Rights and Accessing Records
Records Management Policy
Freedom of Information Policy
Data Protection by Default and Design Standard Operating Procedure
Data Protection Impact Assessment Policy
Standard Operating Procedure for Personal Data Breach Reporting
Standard Operating Procedure for Managing information assets and data flows on the Information Asset Register
General Security Policy
Policy for Risk Identification and Management
Emergency Planning, Resilience and Response Policy
Incident Management Reporting Policy
Duty of Candour Policy
Email Policy
Information Security Response Plan
Internet Usage Policy
Mobile Computing Security Standard
Information Requests and Redaction Standard Operating Procedure
Safe Use of Mobile Phones at Work Policy
Social Media SOP
Standard Operating Procedure for Digital Solutions to accessing visit information
Remote Working Standard Operating Procedure
Adoption Record Protocol
Password Protection Protocol
Media SOP

7. TRAINING

It is compulsory for all new starters to complete onboarding prior to commencement in their post. Onboarding provides new employees with a data protection and security induction.

Managers must complete a local induction checklist with new starters. The local induction checklist requires managers to inform staff about the importance of information governance, information governance training requirements and to provide copies of the Information Governance Policy and Data Protection and Confidentiality Policy. Compliance with onboarding and the local induction checklist will be monitored through Education and Workforce Committee.

Staff are required to complete the Trust's information governance training annually (e-Learning for Healthcare Data Security Awareness Level 1) through ESR.

Information governance training is mandatory for all staff that have access to Trust information.

Managers with management responsibility for staff will be responsible for monitoring staff compliance with e-Learning for healthcare Data Security Awareness Level 1 and for ensuring that staff have sufficient time to complete training.

Bespoke information governance training will be provided by the Information Governance Lead on request by managers that have identified a training need within their team.

Staff with specialist roles are required to complete additional data security and protection training suitable to their role. Additional training requirements will be identified through the annual Training Needs Analysis.

Compliance with mandatory annual information governance training and training for staff with specialist roles will be monitored by the Information Governance and Data Security Group.

8. CONSULTATION

This policy has been reviewed by the Information Governance and Data Security Group prior to submission to the FPC.

9. DISTRIBUTION

The Information Governance Policy will be made available to all staff via Staff Zone. Staff will be informed of the release of this policy through internal communications channels.

10. MONITORING

The Information Governance Lead will annually self-assess the Trust against the assertions set out in the DSPT. Submission of the DSPT will be audited by internal audit. The SIRO is required to sign off both the DSPT and internal audit's final report.

Designated leads will review reported information governance and record keeping incidents and when required the Information Governance Lead will conduct an SBAR or RCA investigation. In the event of an SBAR or RCA investigation a service level action plan will be produced and monitored by the Information Governance and Data Security Group.

The Information Governance Lead will conduct spot check audits as per the DSPT to ensure that staff are adhering to the Information Governance Policy and associated policies and procedures.

The Information Governance Lead is responsible for monitoring, reviewing, and updating the Information Governance Policy on a 3 yearly basis or sooner if the need arises.

11. EQUALITY IMPACT ASSESSMENT

See Equality Impact Assessment in Appendix A.

12. REFERENCES

ARMA International. (2017) *General Accepted Recordkeeping Principles*. Available from: https://www.armavi.org/docs/garp.pdf

Department of Health and Social Care. (2003) *Confidentiality: NHS Code of Practice*. Available from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf

NHS England. (2023) *Records Management Code of Practice.* Available from https://transform.england.nhs.uk/media/documents/NHSE_Records_Management_CoP_2023.pdf

National Cyber Security Centre. (2024) *Cyber Assessment Framework.* Available from https://www.ncsc.gov.uk/collection/cyber-assessment-framework

National Data Guardian. (2013) *Information: To Share or Not to Share? The Information Governance Review.* Available from https://www.gov.uk/government/publications/the-information-governance-review

NHS Digital. (2018) *Data Security and Protection Toolkit Key Roles and the DPO*. Available from: https://www.dsptoolkit.nhs.uk/Help/2

UK Caldicott Guardian Council. (2017) A *Manual for Caldicott Guardians.* Available from https://www.ukcgc.uk/manual/contents

National Data Guardian. (2020) *The Eight Caldicott Principles.* Available from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/942217/Eight_Caldicott_Principles_08.12.20.pdf

Appendix A: Equality Assessment

To be completed at the end of the policy. Write up prior to being submitted for approval.
If you are unsure and would like advice, please contact the Equality & Diversity Manager – wcnt.inclusion@nhs.net

Title	Information Governance Policy Version 5	
What is being considered?	This policy establishes the Trust's information governance framework, sets out high level information governance principles required to ensure compliance with legislation, effective management, and protection of organisational and personal information, and sets out responsibilities and reporting lines for staff.	
Who may be affected?	Patients [x] Staff [x] Public [x] Partner agencies [x]	
Is there potential for an adverse impact against the protected groups below? Age, Disability, Gender Reassignment, Marriage and Civil Partnership, Pregnancy and Maternity, Race, Religion and Belief, Sex (gender), Sexual Orientation or the Human Rights articles?		Yes [ ] No [x]

On what basis was this decision made? (Please complete for both 'yes' and 'no').
All Trust employees and partner agencies are expected to adhere to the Information Governance principles set out in this policy to ensure compliance with legislation and effective management and protection of both organisational and personal information.
For example, you may wish to consider or refer to the some of the following:

- National Guideline / Report (DH / NICE / NSPA / HSE / other)
- Engagement feedback
- Previous Equality Impact screening
- Trust Committee / Multi Agency meeting

If 'No' equality relevance, sign off document below and submit this page when submitting your policy document for approval. If 'Yes,' Please complete pages 2-3.
With regard to the general duty of the Equality Act 2010, the above function is deemed to have no equality relevance.

Equality relevance decision by Anna Simpson Title / Committee FPC Date 01/08/2024

Appendix B: Monitoring Compliance with the process described in the policy.

Minimum requirement to be monitored	Process for monitoring (e.g. audit)	Responsible individual / group/ committee	Frequency of monitoring	Evidence	Responsible individual for development of action plan	Responsible committee for monitoring of action plan and Implementation
Annual completion of DSPT and internal audit	Email evidencing submission Audit	Information Governance and Data Security Group	Annual	Email evidencing submission Audit report	Information Governance Lead and Head of IT	FPC
Annual staff compliance with E Learning for Health Care Data Security Awareness E Learning	BI report	Information Governance and Data Security Group	Monthly	BI report	Head of Data and Electronic Records and Information Governance Lead	FPC
Up to date policies and procedures	Report	Information Governance and Data Security Group	Bimonthly	Information Governance and Data Security Group action log	Information Governance Lead and Chief Digital Information Officer	FPC