Classification Open	Item No.

Meeting:	Audit Committee
Meeting date:	21 July 2021
Title of report:	Information Governance Update 2021/22 Quarter 1
Report by:	Lynne Ridsdale – Deputy Chief Executive
Decision Type:	**Council**
Ward(s) to which report relates	**All**

Executive Summary:

Information Governance (IG) is the strategy or framework for handling personal information in a confidential and secure manner to appropriate ethical and quality standards, ensuring compliance with the relevant statutory and regulatory requirements.

It is of paramount importance to ensure that information is efficiently and legally managed, and that the appropriate policies, procedures, guidance and management accountability and structures provide a robust governance framework for information management.

IG within the Council is delivered through a distributed model of responsibility rather than through a specific or dedicated team, with key roles identified and assigned to ensure appropriate oversight and accountability. These roles include for example, the Senior Information Risk Officer (SIRO), the Data Protection Officer (DPO), Information Asset Owners (IAO) and Information Asset Managers (IAM).

The Audit Committee is responsible for providing assurance on the Council's governance (including risk and information governance) and as set out in the Council's Constitution, is required to annually review the IG requirements.

The Information Governance Steering Group will provide assurance on IG within the Council, to the Committee through strategic and operational oversight and delivery of its wide-reaching work programme, which includes compliance with all statutory requirements and annual compliance with the Data Security and Protection Toolkit (DSPT).

This report provides an update to the Audit Committee on the work of the IGSG, the IG work programme and associated activity that has been progressed during the first quarter of 2021/22.

Recommendation(s)

That: The Audit Committee:

- Note the update provided;
- Note the re-establishment of the IGSG and its formal reporting to the Audit Committee;
- Approve the Terms of Reference of the IGSG; and
- Endorse the Information Governance Framework as presented.

Key considerations

1. Introduction

1.1 This report provides an update to the Audit Committee on the Information Governance (IG) work programme and associated activity that has been progressed during the first quarter of 2021/22.

2. Background

2.1 Information Governance (IG) is the strategy or framework for handling personal information in a confidential and secure manner to appropriate ethical and quality standards, ensuring compliance with the relevant statutory and regulatory requirements.

2.2 It is of paramount importance to ensure that information is efficiently and legally managed, and that the appropriate policies, procedures, guidance and management accountability and structures provide a robust governance framework for information management.

2.3 IG within the Council is delivered through a distributed model of responsibility rather than through a specific or dedicated team, with key roles identified and assigned to ensure appropriate oversight and accountability. These roles include for example, the Senior Information Risk Officer (SIRO), the Data Protection Officer (DPO), Information Asset Owners (IAO) and Information Asset Managers (IAM).

2.4 The Audit Committee is responsible for providing assurance on the Council's governance (including risk and information governance) and as set out in the Council's Constitution, is required to annually review the IG requirements.

2.5 The Information Governance Steering Group (IGSG) will provide assurance on IG within the Council, to the Committee through strategic and operational oversight and delivery of its wide-reaching work programme, which includes compliance with all statutory requirements and annual compliance with the Data Security and Protection Toolkit (DSPT).

2.6 This report provides an update to the Audit Committee on the work of the IGSG, the IG work programme and associated activity that has been progressed during the first quarter of 2021/22.

3. Information Governance Update 2021/22 Quarter 1

3.1 The following updates are provided in respect to the overall work programme:

- **Data Security and Protection Toolkit**

3.2 The Data Security and Protection Toolkit (DSPT) is an online tool that allows relevant organisations that process health and care data to measure their performance against the National Data Guardian's 10 data standards.

3.3 All organisations that have access to NHS patient data and systems must use this Toolkit to provide assurance that they are practicing good data security and that personal information is handled correctly. This is reflected in the Information Standards Notice DCB0086 Amd 9/2019.

3.4 For the 2020/21 reporting period, the submission deadline was 30 June 2021. Ordinarily this is 31 March each year, however due to national, regional and local response requirements to Covid-19, there has been an extended timeframe for both the 2019/20 self-assessment and the 2020/21 self-assessment submission.

3.5 The DPST sets out a number of statements / requirements, some of which are mandatory, which the organisation must confirm, or otherwise, its compliance with, through the provision of a written narrative and / or supporting evidence.

3.6 For the 2020/21 submission, confirmation was provided as follows:

- 44 of 44 mandatory evidence items provided; and
- 39 of 40 assertions confirmed.

3.7 A submission was not made in respect to the specific requirement to provide evidence of an attendance record of a process review, as this was not available at the time of submission.

3.8 The overall submission and published status of the DPST reflected a Standards Met level of compliance.

3.9 A review of the 2021/22 requirements and emerging actions will be incorporated into the IG workplan once released.

- **Information Governance Steering Group**

3.10 There has previously been an Information Governance Group in place, however the work of the group slowed down in 2019 and reduced further during the local response to Covid-19 as resources were redirected.

3.11 Recently, a refreshed Information Governance Steering Group (IGSG) has been established to oversee the IG work programme. This met formally on 28 May 2021, with a subsequent meeting on 15th June 2021 and a regular programme of monthly meetings has been scheduled.

3.12 The IGSG provides the strategic oversight of the IG agenda, and will work closely with the Information Asset Owners, which meet as part of the Strategic Leadership Group, in order that responsibilities for the Information Governance agenda and requirements of the DSPT are shared and more widely understood at a departmental level.

3.13 The IGSG will report to the Audit Committee on a quarterly basis. The Terms of Reference are included at Appendix A for approval having been considered by the IGSG.

- **GDPR Internal Audit**

3.14 In March 2020, the Internal Audit team undertook a review to ensure that appropriate arrangements are in place to ensure that the Council complies with the GDPR legislation. As a consequence of redirecting resources to support the Covid-19 response and changes in resources supporting the information governance agenda, the final draft report was prepared in November 2020.

3.15 The Audit focused on seven specific areas and made 24 recommendations for improvement. The overall audit opinion was assessed as moderate which reflects that there are significant weaknesses in the framework of governance, risk, management and control such that it could be or could become inadequate and ineffective.

3.16 In response to the report and reflecting on the requirements of the DPST and the anticipated Information Commissioner's Office (ICO) audit, an Information Governance Framework and supporting implementation and action plan was developed and discussed with the Executive Team. The Information Governance Framework is attached at Appendix B.

3.17 Good progress is being made against all the actions; however, it should be noted that whilst the programme of improvement and delivery can be addressed in the immediate to short term, it will take some time to embed in day-to-day practice.

- **Information Commissioner's Office review**

3.18 In 2019, Bury Council invited the Information Commissioner's Office (ICO) to undertake a supportive review and audit of the Council's IG arrangements in place to ensure the organisation's compliance with the GDPR. The review was due to take place in May 2020 but was deferred due to the pandemic, and rearranged for June 2021.

3.19 The review considered three specific areas in respect to Governance and Assurance, Information Security and Freedom of Information and comprised of an initial desk-top assessment which was then followed up with a three-day virtual on-site assessment and series of interviews with colleagues across the organisation.

3.20 Feedback provided at the end of the assessment reflected some areas of good practice across all areas and also reflected similar recommendations as identified through the Internal Audit and as captured in the workplan developed to support the implementation of the Information Governance Framework.

3.21 A final detailed report and action plan from the review will be provided to the Council no later than 30 July 2021. All findings will be reviewed and incorporated into the existing IG workplan.

- **Information Governance Framework**

3.22 The Information Governance Framework, as a comprehensive policy document, sets out the core components required to deliver effective information governance practice through all our activities. Updates against each of the areas are provided below:

- Strategy

3.23 The overarching Information Governance Framework is currently the strategy document and has been approved. This is supported by a comprehensive implementation plan which is monitored through the Information Governance Steering Group.

- Governance

3.24 Arrangements to support good governance have been refreshed, including the IGSG which will be supported in terms of delivery through the Strategic Leadership Group and Senior Manager Forum, both of which were existing meeting forums. The network of IG champions across the organisation is also being refreshed.

- Roles and Responsibilities

3.25 Work has been progressed to confirm the Information Asset Owners (IAO) across each area in the Council. The IAOs will work in collaboration with the SIRO and DPO as well as their Information Asset Managers (IAMs).

- Policy

3.26 A number of data protection and information governance policies have been refreshed and approved by the portfolio holder in accordance with the scheme of reservation and delegation:

  - Data Protection Policy v3.0
  - Records Management and Disposal Policy v2.0
  - Bury ICT Data and Network Security Policy v2.0
  - Information Security Policy v2.0

3.27 A full policy schedule has been drafted and policies will be prioritised for review and refresh accordingly.

- Standards, including Training

3.28 A training needs analysis has been completed which identified both the generic and role specific training that needs to be delivered across the organisation.

3.29 Requirements to complete the GDPR training on an annual basis have been reconfirmed and each department has made significant progress in securing completion of this training by 95% of colleagues in the last 12-month period.

3.30 Work is progressing on commissioning the additional training required for specific roles.

- Procedures and Guidelines

3.31 IAO's have been tasked with ensuring that the Record of Processing Activity (ROPA), Information Asset Registers (IAR) and Data Flow Mapping (DFM) for their respective areas are up to date.

3.32 Additionally, mapping of the Freedom of Information (FoI) and Subject Access Request (SAR) procedure has also commenced. This will be presented to the next Information Governance Steering Group and will be supported by refreshed policies, training and monitoring arrangements.

4 Recommendations

4.1 The Audit Committee is required to:

- Note the update provided;
- Note the re-establishment of the IGSG and its formal reporting to the Audit Committee;
- Approve the Terms of Reference of the IGSG; and
- Endorse the Information Governance Framework as presented.

Other alternative options considered

None.

Community impact / Contribution to the Bury 2030 Strategy

Good Information Governance practices enables the Council to deliver its statutory requirements and therefore contributes across all the themes of the Bury 2030 Strategy.

Equality Impact and considerations:

24. *Under section 149 of the Equality Act 2010, the 'general duty' on public authorities is set out as follows:*

A public authority must, in the exercise of its functions, have due regard to the need to -

(a) *eliminate discrimination, harassment, victimisation and any other conduct that is prohibited by or under this Act;*

(b) *advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it;*

(c) *foster good relations between persons who share a relevant protected characteristic and persons who do not share it.*

25. *The public sector equality duty (specific duty) requires us to consider how we can positively contribute to the advancement of equality and good relations, and demonstrate that we are paying 'due regard' in our decision making in the design of policies and in the delivery of services*.

Assessment of Risk:

The following risks apply to the decision:

Risk / opportunity	**Mitigation**
Without a robust framework in place to support good Information Governance practice, there is a risk that the Council may not comply with the duties set out in the General Data Protection Regulations (GDPR) 2018 or Data Protection Act leading to possible data breaches, loss of public confidence, reputational damage and prosecution / fines by the Information Commissioner	Approval and Implement of the Information Governance Framework Implementation of a comprehensive Information Governance work programme

---

Consultation: N/a

Legal Implications:

The report references the Council's statutory duties and obligations under the UK GDPR, Data protection Act 2018, FOIA and associated legislation and guidance. The Council has duties under this legislation in terms of accountability and compliance and must ensure it has appropriate policies and procedures in place. A Failure to ensure compliance could result in enforcement action by the ICO.

Legal advice and support will be required in terms of the action plan outlined in the report as well as ongoing DPO oversight and support.

Financial Implications:

With the exception of the procurement of appropriate training there are no direct financial implications arising from this report. However, there are implications in relation to a potential ICO fine if the Council had a data breach and the ICO found that we as an organisation were negligent.

Report Author and Contact Details:

Lynne Ridsdale – Deputy Chief Executive

l.ridsdale@bury.gov.uk

Background papers: N/A

Please include a glossary of terms, abbreviations and acronyms used in this report.

Term	Meaning
DFM	Data Flow Mapping
DPO	Data Protection Officer
DPST	Data Security and Protection Toolkit
FOIA	Freedom of Information Act 2000
GDPR	General Data Protection Regulations 2018
IAM	Information Asset Manager
IAO	Information Asset Owner
IAR	Information Asset Registers

ICT	Information Communication and Technology
IG	Information Governance
IGSG	Information Governance Steering Group
NHS	National Health Service
ROPA	Record of Processing activity
SAR	Subject Access Request
SIRO	Senior Information Risk Officer

Appendix A

TERMS OF REFERENCE

INFORMATION GOVERNANCE STEERING GROUP

Terms of Reference Document Control Sheet

MEETING	Information Governance Steering Group

Version Control

Version Ref	Amendment	Date
V0.1	Initial draft prepared for discussion	May 2021
V0.2	Updated following discussion at IGSG	May 2021

1.0 Introduction

1.1 The Information Governance Steering Group (IGSG) is a key element of the organisations approach to good information governance practice.

1.2 The IGSG is established with a reporting line to the Audit Committee, which in accordance with Bury Council's constitution, standing orders and scheme of delegation, has responsibility for assuring the Information Governance activity of the Council.

1.3 These terms of reference set out the membership, remit, responsibilities and reporting arrangements of the IGSG.

1.4 The IGSG is established to oversee and influence the development of Information Governance, Data Protection and Security across Bury Council, including associated independent contractors and service providers, via the implementation of an Information Governance Framework.

1.5 The IGSG will also provide assurance on the Council's statutory requirements in relation to information governance and associated legislation and Department of Health and Social Care requirements, including the completion of the Data Security and Protection Toolkit (DSPT).

1.6 Any changes to these Terms of Reference must be approved by the Audit Committee

2.0 Membership

2.1 The IGSG membership will include a balance of skills, knowledge, experience and interests to ensure that it can discharge its delegated duties.

- SIRO (Chair)
- DPO (Vice Chair)
- Caldicott Guardian – Adults
- Caldicott Guardian - Children
- Deputy Director Governance and Assurance
- Chief Information Officer
- Information Governance Project Officer

2.2 The IGSG may at its discretion invite attendees to its meetings to support it in discharging its duties and purpose.

2.3 The IGSG will direct its work through the specialist roles and with co-operation from the Strategic Leadership Group and Senior Manager Form.

3.0 Attendance

3.1 Members should attend all meetings however it is expected that members will normally attend a minimum of 75% of meetings held per annum.

3.2 Should a member not be able to attend a IGSG meeting, apologies in advance must be provided to the Chair.

3.3 In those cases where a member cannot attend, a deputy should be discussed and agreed with the chair who will attend on a member's behalf and is empowered to make judgements and decisions accordingly. Any formal acting up status will be recorded in the minutes.

4.0 Quorum

4.1 The meeting will achieve quorum if at least four members are present which must include the Chair or Vice Chair.

5.0 Frequency

5.1 The IGSG shall meet monthly with all meetings being undertaken virtually.

5.2 The agenda and supporting papers for each meeting will be issued at least five working days before the meeting.

6.0 Duties

6.1 The purpose of the IGSG is to oversee and influence the development of Information Governance, Data Protection and security agenda across the organisation which will include, but is not limited to:

- oversee the implementation of the General Data Protection Regulations;
- share new initiatives and case law and produce briefings for staff and management teams on their meaning and required application;
- approve and ensure a comprehensive information governance framework, policies, standards, procedures and systems are in place and operating effectively;
- Oversight and approval of all annual Information Governance / Risk Assessment required, including action plans and the annual submission of compliance with the requirements in the Data Security and Protection Toolkit;
- oversee the development of information sharing agreements;
- promote the Information Sharing Gateway for recording and monitoring information sharing across partnerships;
- act as an advisory group on implications /developments of information governance when setting up systems and projects;

- Oversight of legislation and operational requirements for Information Governance activities (data protection, information requests, information security, quality, and records management);
- Ensure any identified gaps in processes / procedures that may have implications for Information Governance;
- Ensuring there are clear links with the ICT information security policies and procedures.
- Monitor information handling and data breaches, implementing assurance controls (including Data Protection compliance audits as required) and taking corrective actions and share the learning from these;
- Ensuring that Information Risk Management forms an integral part of Information Governance agenda.
- Ensure training and action plans for information governance are progressed and evaluate the impact and effectiveness of training; and
- Develop and oversee the communication plan that supports the information

7.0 Reporting

7.1 The IGSG meeting will be formally noted and a summary note of business undertaken by will be submitted to the Audit Committee on a quarterly basis.

8.0 Monitoring Compliance

8.1 The IGSG will develop an annual work plan with specific objectives which will be reviewed regularly and formally on an annual basis.

8.2 The IGSG will produce an annual report to reflect progress against the workplan, which will include a baseline and final assessment against the DPST.

9.0 Reviewing Terms of Reference

9.1 The Terms of Reference of the IGSG (including membership) shall be reviewed at least annually.

INFORMATION GOVERNANCE FRAMEWORK
2021-22

Further information regarding this document

Document name	Information Governance Framework	
Author(s) Contact(s) for further information about this document	Lisa Featherstone, Deputy Director	
This document should be read in conjunction with	Insert the names and numbers of any policies which should be used in conjunction with this document	
Supersedes	Data Protection and Security Framework v7.0 (CCG) TBC (Council)	
This document has been developed in consultation with	Data Protection Officer, Bury Council Director of Corporate Core Services, Bury Council	
This document has been ratified by		
This document will be reviewed in	12 months	
Published by	**NHS Bury CCG** Townside Primary Care Centre 1 Knowsley Place, Knowsley Street, Bury, BL9 0SN www.buryccg.nhs.uk	**Bury Council**

Version Control

Version	Date	Reviewed by	Comment
v0.1	30/12/2020	Deputy Director Governance and Assurance	Initial draft submitted for wider review
v0.2	11/01/2021	Deputy Director Governance and Assurance	Table at 3.2 updated
v0.3	April 2021	Reviewed by ET	Supported
V0.4	28 May 2021	Reviewed by IGSG	Supported
v1.0	04 June 2021	Audit Committee	Approved and Ratified

Contents

1.0 Introduction

1.1 Information is a key corporate asset that requires the same discipline to its management as is applied to other important corporate assets such as finance, people and facilities, to enable better decision making and delivering effective services to our communities, residents, service users, patients and staff.

1.2 Through the day-today operation of the CCG and Council access, store and create a wide range of information and data in many different formats.

1.3 It is therefore imperative to ensure an effective framework for collecting, accessing, storing, sharing and deleting information across all services, that is sufficiently robust, consistently applied and statutorily compliant is in place.

1.4 This Information Governance Framework outlines our approach to the effective management of information and data through the identification of key roles and responsibilities and development of policies and procedures, along with best practice and standards for managing the information assets.

1.5 This IG Framework, which has been developed to take account of the standards set by the Information Commissioners Office and other relevant legislation and guidance, is an essential element of the wider corporate governance agenda and interlinks with other governance arrangements such as audit, risk, business continuity and information technology / digital management.

2.0 Purpose and Scope

2.1 Good information management is vital to ensure the effective and efficient operation of services, the meeting of standards and compliance with legislation and for demonstrating accountability for decisions and activities.

2.2 This framework therefore applies to all CCG and Council employees and all individuals or organisations acting on behalf of the CCG and / or Council.

2.3 The framework is not directly applicable to schools or GP practices who remain data controllers in their own right, however it can be called upon as needed, along with other underpinning IG policies to support and enable the discharge of duties.

2.4 Through the implementation of the Information Governance Framework the CCG and Council aims to:

- strategically and actively manage information as a critical business asset;
- understand the information available, needed and retained, including sensitive, restricted, personal or special class information;

- ensure that all information is complete, accurate, accessible and useable by those with a legitimate need and legal basis;
- establish, implement and maintain local policies, procedures and guidelines that comply with legislative and regulatory requirements to enable the effective management of data processed;
- effectively manage the storage and security of information;
- ensure information is publicly accessible and provide clear guidance about how information is recorded, handled, stored, shared and managed to promote transparency;
- provide clear advice, guidance and training to all staff, irrespective of contractual status, to ensure that they understand and apply the principles of robust information governance to their working practice;
- develop and sustain an Information Governance culture through increasing awareness and promoting good information governance practice thus minimising the risk of breaches;
- assess corporate performance using the Data Security and Protection Toolkit and Internal Audits, developing and implementing action plans to ensure continued improvement as required.

2.5 The benefits of the framework will be:

- increased efficiency through the more effective use of physical, electronic and human resources;
- better service delivery through improved access to relevant information making requests easier to handle in a shorter time and in line with statutory timeframes where applicable;
- contribution to improved environmental benefits by reducing reliance on paper files and physical storage;
- more agile working through the removal of irrelevant information and documentation from static office bases with a shift to cloud-based retention of essential documentation allowing staff easier access to the information required to perform their work; and
- improved compliance with legal requirements through promotion of positive Information Governance culture which instils corporate and public confidence, building a credible reputation as a data controller.

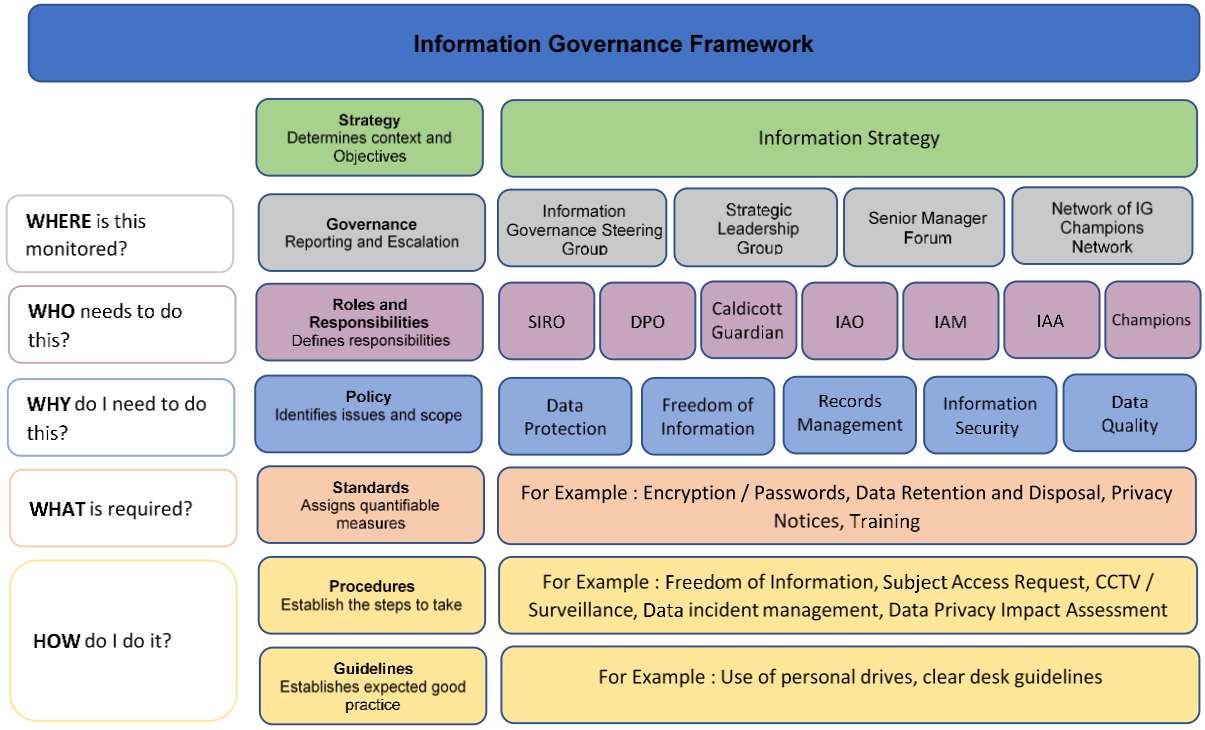
2.6 The Framework and the underpinning strategies are based upon the following standards and legislation that apply to information governance and management:

Data Protection Act 2018	Health and Social Care Act 2012	Freedom of Information Act 2000	•General Data Protection Regulation 2018 (GDPR);	A Guide for Confidentiality in Health and Social care
Common Law Duty of Confidentiality	Caldicott Guidance	Access to Health Records Act 1990	Public Records Act 1958	Environmental Information Regulations 2004
Regulation of Investigatory Powers Act 2000	Re-use of Public Sector Information Regulations 2005	Local Government Act 2000	•Code of Recommended Practice for Local Authorities on Data Transparency (2011)	•Computer Misuse Act 1990
•Huiman Rights Act 1998	•Information Security NHS Code of Practice	•Information Security Standard ISO 27002:2005	•Records Management code of Practice for Health and Social Care 2016	•Mental Capacity Act 2005
•NHS Constitution – Department of Health	•NHS Data Security andProtection Toolkit (DSPT)	•ICO guidance and good practice	•Notification of Data Security and Protection incidents (May 2018)	•Openness of Local Government Bodies Regulations 2014

3.0 Information Governance Framework

3.1 Information Governance is about ensuring that organisational information is managed as an asset to ensure that all statutory, regulatory and best practice requirements are met.

3.2 Our approach is set out in the diagram below:



3.3 All supporting policies, standards, procedures and guidelines will be made available through the shared drives and intranet.

4.0 Key Roles and Responsibilities

4.1 Information Governance is the responsibility of all employees and contractors working on behalf of the CCG and / or Council and willful or negligent disregard for information governance policies and procedures will be investigated and may be treated as a disciplinary matter which could lead to dismissal or the termination of work agreement or service contracts.

4.2 The following specific roles and responsibilities are applicable in respect to this Framework:

Accountable Officer / Chief Executive

4.3 The Accountable Officer / Chief Executive has overall responsibility for Information Governance of both the Council and CCG, which includes the effective management through appropriate mechanisms which support service delivery and continuity.

Senior Information Risk Officer (SIRO)

4.4 The SIRO (Executive Director of Finance) has responsibility for information as a strategic asset of the organisation and ensuring that the value of this asset to the organisation is understood and recognised and that measures are in place to protect against risk.

4.5 The SIRO has a key role in ensuring that the organisation:

- identifies and manages its information risks;
- implements robust information asset management arrangements;
- reviews and agree actions in respect of identified information risks; and
- ensures sufficient resources are in place to manage the information governance agenda.

4.6 The SIRO is supported by the Deputy Director of Governance and Assurance who acts is a 'designate SIRO' capacity for all day-to-day matters.

Data Protection Officer (DPO)

4.7 The GDPR introduces a legal duty for all public authorities and organisations that carry out certain types of processing activities to appoint a Data Protection Officer (DPO).

4.8 DPOs assist to monitor internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments, (DPIAs) and act as a contact point for data subjects and the supervisory authority (ICO).

4.9 The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level.

4.10 There will be respective DPOs within both the CCG and Council, and where required additional DPO resource will be commissioned to support General Practice in accordance with the standard GP contract requirements and management of conflicts of interest.

Caldicott Guardian

4.11 The Caldicott Guardian(s) are responsible for protecting the confidentiality of people's health and care information and for making sure it is used properly. They will act as an advocate for information sharing at a strategic level and in internal discussions. Key tasks will include:

- Ensuring that the organisation and its partner organisations satisfy the highest practical standards for handling patient and service user information;
- Acting as the 'conscience' of the organisation in relation to information sharing and supporting work to enable information sharing where it is appropriate to do so; and
- Advising on options for lawful and ethical processing of information.

4.12 There will be an identified Caldicott Guardian for Adult, Children and OCO health and care commissioning.

Chief Information Officer (CIO)

4.13 With the development of the digital agenda, greater emphasis has been incorporated into statutory requirements on Cyber and Data Security. The Chief Information Officer (CIO) oversees the arrangement sin both organisations through either direct of commissioned provision for the security of networks, including remote working facilities and ensuring effective controls are in place.

Information Governance Manager

4.14 Working under the direction of the Deputy Director Governance and Assurance (designate SIRO), the Information Governance Manager is responsible for ensuring the day-to-day delivery of the Information Governance agenda, including oversight and delivery for all aspects of Data Security and Protection Toolkit.

4.15 The IG Manager will ensure that in addition to internal relationships with identified IG post holders, they will also foster good relationships across Greater Manchester in respect and specifically with the NHS GM IG Group and GMCA Senior IG Lead and ensure any regional guidance is reflected into local practice as necessary.

Information Asset Owners

4.16 The Information Asset Owners (IAO) are senior members of staff who understand the overall business goals of the organisation and how the information assets they own contribute to and affect these goals. An Information Asset is any form of information that has a value to the organisation (for example personal development plans, or complaint records) and is recorded on a departmental Information Asset Register (IAR).

4.17 Deputy and / or Assistant Directors, or equivalent have been identified as IAOs.

Information Asset Managers

4.18 The Information Asset Managers (IAM) have day to day management responsibility of the information assets used in their business area. They usually use them more frequently than an IAO and can identify the risks associated with the assets they use and how to ensure continued compliance with legislation.

4.19 Heads of Service have been designated as IAMs

Information Asset Administrators (Champions)

4.20 All employees and individuals working on behalf of the Council and / or CCG are Information Asset Administrators (IAA) and have a responsibility to be the 'eyes and ears' that help keep the organisation safe and compliant, report when things may have gone wrong, keep asset registers up-to-date and highlight information risk, issues and concerns as they emerge. The IAAs are collectively responsible to achieving Information Governance success.

Information Governance Champion

4.21 Each area will identify an Information Governance Champion, who take an active role, working alongside the IAO, IAM and IAAs to ensure that the information governance agenda is enabled through day-to-day operations. The IGCs will be supported to increase their knowledge and understanding of information governance related activity and will act as a departmental expert and advocate for good information governance practice.

5.0 Governance and Reporting Arrangements

5.1 To support the delivery of the Information Governance Framework, two delivery groups will be established.

5.2 An Information Governance Steering Group (IGSG) will bring together strategic leads who support the Information Governance agenda, including the SIRO, designate SIRO, Data Protection Officer(s), Caldicott Guardian(s), Chief Information Officer (CIO), Information Governance Manager and other representatives from each department as required, and has a remit to:

- Approve and ensure a comprehensive information governance framework, policies, standards, procedures and systems are in place and operating effectively;
- Oversight and approval of all annual Information Governance / Risk Assessment required, including action plans and the annual submission of compliance with the requirements in the Data Security and Protection Toolkit;
- oversee the development of information sharing agreements;
- promote the Information Sharing Gateway for recording and monitoring information sharing across partnerships;
- act as an advisory group on implications /developments of information governance when setting up systems and projects;
- Oversight and coordination of Information Governance activities (data protection, information requests, information security, quality, and records management);

- Monitor information handling and breaches, implement assurance controls (including Data Protection compliance audits as required), take corrective actions and share the learning from these;
- Ensure training and action plans for information governance are progressed and evaluate the impact and effectiveness of governance training; and
- Oversee the communication plan that supports the information governance agenda

5.3 In addition, the Strategic Leadership Group(SLG) and Senior manager Forum (SMF) will bring together the Information Asset Managers to ensure all operational aspects of information governance are progressed and compliance with required internal and external assessments (e.g. internal audits, DPST) including:

- Identify gaps in processes/ procedures that may have implications for Information Governance;
- Establishment of Information Asset Registers and Data Flow mapping across all teams;
- Keep under review Information Asset Registers by department;
- Keep under review Data Flow Mapping registers by department;
- Keep under review Record of Processing Activities (ROPA);
- Keep under review and co-ordinate DPIA and DSA registers;
- Oversee delivery of actions arising from data breaches;
- Provide updated on departmental performance in respect to SARs and FOIs; and
- Contribute to and prepare compliance reports with annual assessments and audits.

5.4 The Information Governance Manager will also bring together the network of Information Governance Champions to support continued improvements in the wider application of Information Governance across all teams.

6.0 Dissemination, Implementation and Training

6.1 The framework will be communicated to all staff through corporate communication channels and will be mandated as part of every new starter induction, and periodically thereafter in line with the corporate training standard for information governance, whether employed, elected, contracted or working on a voluntary basis.

6.2 A Training Needs Analysis will be completed annually, and all staff and Elected Members will receive training consummate with their roles and responsibilities around information handling, management and cyber security.

6.3 As a minimum all staff are required to complete the mandatory IG module using the agreed method detailed in the approved Training Needs Analysis, however further modules for specific information governance and / or certain business roles will be available through e-learning and / or classroom sessions, developed internally or through recognised providers, as required. The requirements and standards for these will be developed, agreed and kept under review.

6.4 The SIRO, Caldicott Guardian(s), DPO, IG Manager, Information Asset Owner's (IAO) and Information Asset Managers (IAMs) must complete relevant additional training.

6.5 Training compliance will be monitored by the Information Governance Steering Group (IGSG) and at an individual employee level through the annual appraisal process.

6.6 Awareness sessions may be given to staff as required, at team meetings or other events.

6.7 Regular reminders on information governance topics will be delivered through corporate and team briefings, staff newsletters and e-mail communication.

6.8 Failure to comply with Information Governance training requirements will be managed in accordance with agreed policies.

7.0 Monitoring and Review

7.1 The Information Governance Framework will be monitored and reviewed annually in line with legislation and codes of good practice.

7.2 The policies, procedures, standards and guidance that form part of the Framework will be reviewed as set out in the individual documents.

7.3 A detailed review and change log of all documents which comprise this Framework will be maintained by the Information Governance Manager.

8.0 Other related documents

8.1 This Framework should be read in conjunction with the suite of other Information Governance Policies, procedures and guidelines.