Nottinghamshire County Council

Information Governance Framework

Introduction

1. Information is a vital asset for the provision of services to the public and for the efficient management of Council services and resources. It plays a key part in governance, service planning and delivery as well as performance management.

2. "*Governance is about how the County Council ensures it is doing the right things, for the right people, in the best way, in a timely, inclusive, open and accountable manner.*"

3. Information governance is concerned with how information is held, obtained, recorded, used and shared. Information is used here as a collective term to cover things such as data, documents, records and content (electronic and paper).

4. It is essential that the Council has a robust information governance framework, to ensure that information, particularly personal, special category, sensitive and confidential information, is effectively managed with accountability structures, governance processes, documented policies and procedures, staff training and appropriate resources.

Scope

5. The principles and commitments set out in this Framework and associated documents apply to all members, employees, trainees / apprentices and volunteers of the County Council and to contractors, suppliers and partners delivering services on the Council's behalf.

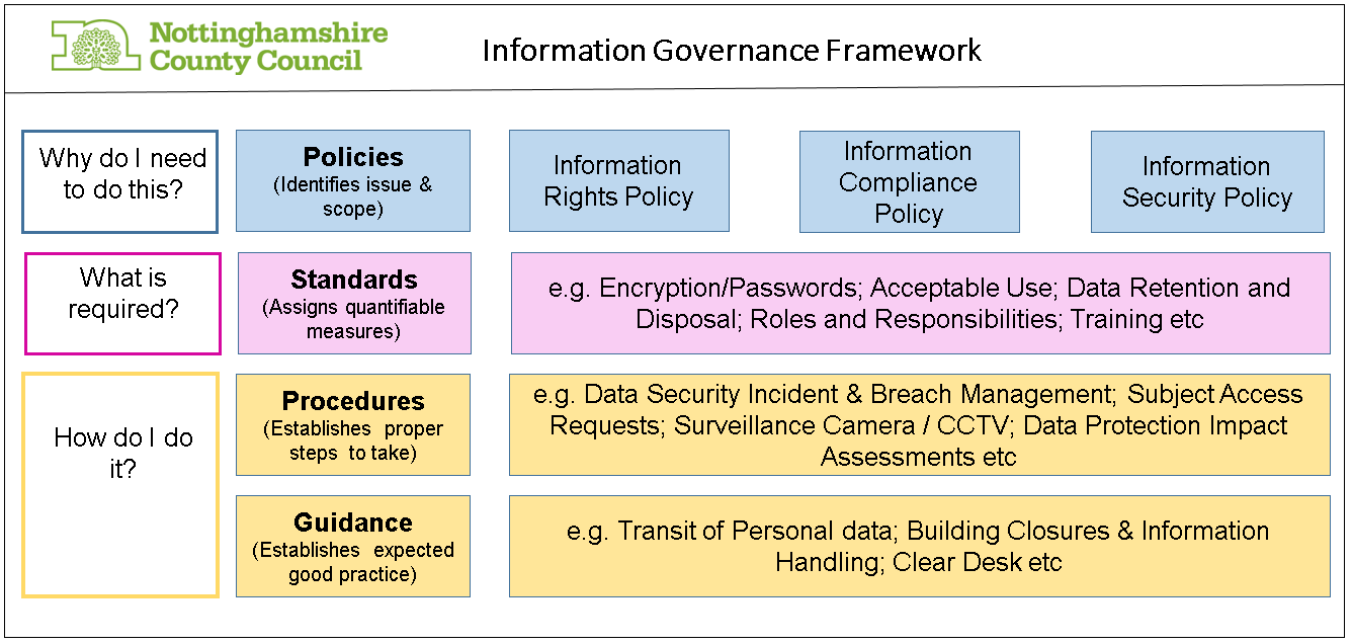
6. This Framework and associated documents do not apply to schools who are individually responsible for ensuring that they comply with Data Protection and Freedom of Information legislation.

Key policies

7. The key policies in this information governance framework are the:

   - **Information Rights Policy** – aimed at the public
   - **Information Compliance Policy** – aimed at all staff
   - **Information Security Policy** – aimed at staff and ICT specialist staff

8. These policies are supported by standards, procedures and guidance which are shown in the framework diagram below.



9. Outputs will be produced from use of these standards and procedures, for example Data Protection Impact Assessments, information awareness guides and training material.

10. The framework and associated policies, procedures and standards can be found in the information governance policy library.

Committees and Elected Members

11. Policy Committee is the lead Elected Member body responsible for decision making in respect of Council policies.

12. Governance and Ethics Committee has responsibility for overseeing performance and compliance in respect of agreed information governance policies. It also has decision making responsibility in respect of the information governance approach and performance.

Senior officer roles

Chief Executive and Corporate Leadership Team

13. The Chief Executive is the Head of Paid Service who leads the Council's staff and advises on policies, staffing, service delivery and the effective use of resources.

14. The Chief Executive, together with Corporate Directors and a few other senior officers, form the Council's Corporate Leadership Team (CLT) ensures the delivery of an effective Council-wide information governance approach.

Senior Information Risk Owner (SIRO)

15. All NHS organisations and local authorities which provide social care must have a Senior Information Risk Owner (SIRO). The SIRO is a member of the Corporate Leadership Team; is responsible for managing information risk in the Council and chairs the Information Governance Board. The SIRO:

- fosters a culture for protecting and using information within the Council
- ensures information governance compliance with legislation and Council policies
- provides a focal point for managing information risks and incidents
- prepares an annual information risk assessment for the Council
- gives strategic direction to the work of the Data Protection Officer (DPO)

Caldicott Guardians

16. All NHS organisations and local authorities which provide social care must have a Caldicott Guardian. Within the Council, both Adult's Social Care and Children's Social Care has a Caldicott Guardian.

17. A Caldicott Guardian is a senior person responsible for protecting the confidentiality of people's health and care information. They also make sure the personal information is used properly, in a way which is compliant with the law and consistent with Caldicott Principles (general principles of information governance designed to be used by all NHS organisations with access to patient / service user information).

Data Protection Officer

18. All public authorities and organisations that collect and use large volumes of personal information must appoint a Data Protection Officer (DPO). A DPO must act independently and is responsible for advising the Council on its data protection obligations; monitoring internal compliance with data protection law; informing and providing advice regarding Data Protection Impact Assessments (DPIAs); investigating data breaches and incidents; and acting as a contact point for individuals with concerns about the way their data has been handled and the Information Commissioner's Office (the UK Regulator for Data Protection).

19. Within the Council, the DPO is also the Senior Responsible Owner for ensuring that the Council uses open surveillance / CCTV cameras in a way which is compliant with relevant legislation and the Surveillance Camera Commissioner's Surveillance Camera Code.

Information Asset Owners

20. Each Service Director is an Information Asset Owner who is accountable for identifying, understanding and addressing risks to the information assets within their directorates as well as ensuring good information governance.

Information Asset Managers

21. Each Group Manager is an Information Asset Manager who is responsible for the information assets and wider information governance within their business unit. They ensure information is held, used and shared appropriately and support the Information Asset Owner to address risks to the information. They also ensure that data breaches are properly investigated and that lessons are learned to reduce / prevent reoccurrence.

Team / Service Managers

22. Each Team or Service Manager understands and records the information assets for their business unit and supports the Information Asset Manager and Owner to address risk and safeguard assets. They also promote good information governance practice amongst their staff including ensuring data breaches are minimised.

23. An Information Governance Roles for Managers role descriptor sets out in more detail the information governance responsibilities for staff at each of these levels of the organisation.

Information Systems Owners

24. All information systems within the Council which collect, store or use personal data will have an assigned System Owner. Systems Owners are responsible for ensuring that system operating procedures (which set out how data is controlled and kept secure) are in place and are followed. They have responsibility to ensure that Data Protection Impact Assessments are in place for the systems they own; to recognise and act on actual or potential security incidents and breaches; to consult relevant Information Asset Owners on incident management; and ensure that data in systems are accurate and up to date.

25. An Information System Owner Role Descriptor sets out in more detail the responsibilities for staff assuming this role.

Key officer governance bodies

Information Governance Group (IGB)

26. The Information Governance Board (IGB) comprises the SIRO (Chair), Caldicott Guardians, the Chair of the Risk, Safety and Emergency Management Board, the Data Protection Officer, senior representatives from Legal Services, ICT and Assurance. The role of the Board is to

- provide leadership to improve the Council's approach to controlling information security and data protection risk.
- ensure that data and information is managed with the same determination and focus as other key business objectives
- ensure legal compliance and embed an information governance culture

Risk, Safety and Emergency Management Board and Groups

27. The Risk, Safety and Emergency Management Board (RSEMB) is the Council's strategic level group for corporate risk management, health and safety, emergency planning & business continuity. The RSEMB ensures the Council is resilient to disruptive challenges by providing leadership and co-ordination of the Council's arrangements in these areas. RSEMB maintains an overview of information governance risk and its chair is a member of the Information Governance Board.

28. Each Department has a Risk, Safety and Emergency Management Group whose role is to consider and address information governance risk within that Department, as part of a wider risk management agenda.

Officer Resources

29. The Council has dedicated resources to support the implementation of its Information Governance Framework. The role these teams play in that regard are briefly set out below.

30. The Information Governance Team provides expert advice, guidance and training to all staff on Information Governance and supports the DPO in their role. The Team coordinates the management and reporting of data incidents and breaches; supports the production of DPIAs and Information Sharing Agreements (ISAs) to minimise information risk; maintains information to evidence compliance with data protection law (e.g. registers of surveillance cameras; submits the annual Data Security and Protection Toolkit etc).

31. The Complaints and Information Team processes information rights requests (e.g. Subject Access Requests (SARs); erasure requests etc), Freedom of Information requests and Environmental Information requests.

32. The IT Security team is the lead for cyber security management and advice for the Council's IT infrastructure, and for the annual IT Health Check for the PSN (Public Sector Network) Accreditation.

33. The Records Management Service is provided by Inspire. It produces and maintains the Council's Data Retention and Destruction Standard and provides records management advice and storage to all departments of the County Council. It controls the quantity and

length of time that paper records are retained by carrying out annual reviews and maintains an audit log of information use.

34. The Solutions 4 Data Service provides a digitisation service which enables paper documents to be scanned and indexed to enable easy retrieval.

35. The Legal Services team provides expert legal advice on data protection law and information governance matters to all service teams, including the Information Governance, Complaints and Information and Information Security teams.

36. The Policy, Intelligence and Performance Team provides advice and guidance on data quality and more technical aspects of data minimisation (i.e. anonymisation and pseudonymisation).

37. The Internal Audit Service provides independent assurance of the Council's approach to risk management, control and governance in order that systems and processes are made more effective.

General responsibilities

38. All Council directors and managers are responsible for promoting and monitoring the implementation and adherence of this Information Governance Framework and its associated standards, procedures and guidance within their directorates and services.

39. All staff are responsible for ensuring they apply this Information Governance Framework its associated standards, procedures and guidance to their work and the information they handle.

40. Wilful 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.

Training and guidance

41. Information Governance training for all staff will be mandatory at induction and periodically thereafter, in line with the corporate training standard for information governance.

42. Secondees, agency, voluntary and other staff with access to Council systems and data will be required to undertake the training in line with requirements of staff unless evidence of equivalent training is provided through an exceptions process.

43. Further modules, as appropriate, for specific information governance and / or certain business roles will be made available. The requirements and standards for these have been developed, agreed and will be kept under review.

44. Training compliance will be monitored by the Information Governance Board and at an individual level through Employee Performance and Development Reviews (EPDRs).

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

46. Regular reminders on information governance topics are made through corporate and local team briefings, staff news and emails and, on occasions, through targeted publicity campaigns.

47. Policies, procedures, standards and advice are available to staff at any time on the Data Protection and Information Governance hub of the Council's intranet.

Monitoring and review

48. This Information Governance Framework will be monitored and reviewed every two years in line with legislation and codes of good practice.

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

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

Appendices

51. The primary appendices of this policy document are the Information Rights; Compliance and Security Polices which can be found in the Council's Policy Library. Each of these polices has a list of standards, procedures and guidance documents which are available at the time of approval.

External Legislation

52. External legislation related to this policy includes:

- General Data Protection Regulation
- Data Protection Act 2018
- Human Rights Act 1998
- Protection of Freedoms Act 2012
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Local Government Acts
- Computer Misuse Act 1990

Further Information

53. Further information, advice or guidance on this document can be obtained from:

The Information Governance Team
By email: data.protection@nottscc.gov.uk
By telephone: 0115 8043800

Document Control

Owner	Data Protection Officer
Author	Caroline Agnew, Data Protection Officer
Last Reviewer	Caroline Agnew, Data Protection Officer
Approver	Senior Information Risk Owner (SIRO) under delegation from Policy Committee
Date of Approval	30/10/2019
Date of next review	29/10/2021
Version	2.0
Classification	Public

Version	Date	Changes
1.0	28/03/18	Original document approved by Policy Committee
2.0	30/10/19	Changes to reflect post-GDPR experience, framework diagram, governance changes, insert links etc. Approved by SIRO under delegation from Policy Committee