Nottinghamshire County Council

Information Governance Framework

Version: 1.0
Author: Caroline Agnew
Date of Issue: 28/03/2018
Review date: 28/03/2019
Protective Marking: Official

Approvals

V1.0	Policy Committee	28/03/2018

Review

V	Reviewing Body	Change Description	Date

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 terms 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 and sensitive 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 County Council services on our behalf.

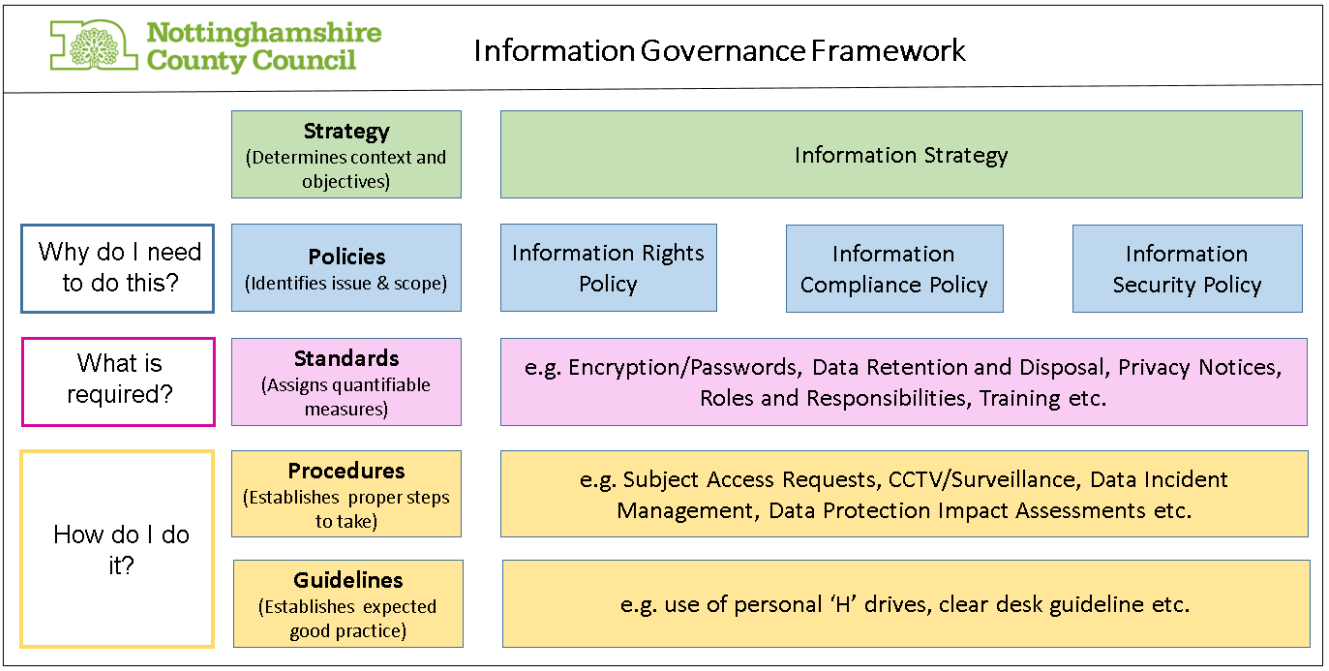
6. This Framework and associated documents does not apply to schools who are individually responsible for ensuring that they comply with Data Protection and Freedom of Information legislation.

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 guidelines 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, awareness guides and training material.

10. The framework and associated policies, procedures and standards can be found at: Information Management and data protection

Senior roles

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 a decision making responsibility in respect of the information governance approach and performance.

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) which ensures the delivery of an effective Council-wide information governance approach.

Senior Information Risk Owner (SIRO)

15. The Senior Information Risk Owner (SIRO) is responsible for managing information risk in the Council and chairs the Information Governance Group. 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. The Caldicott Guardians are responsible for ensuring that all personal/patient identifiable information handled on behalf of the Council, are compliant with existing law and standards and they act to safeguard the rights of service users. The Caldicott Guardian ensures that satisfactory information governance policies are in place for their service and adhered to by all staff and providers in their service area.

Data Protection Officer

17. The Data Protection Officer (DPO) is responsible for advising, monitoring and reporting the Council's compliance with the General Data Protection Regulation (GDPR) and any relevant UK legislation. The GDPR is the EU-wide legislation on data protection which becomes law with effect from 25 May 2018. Formal duties are defined by the GDPR and include raising awareness of data protection requirements, leading information audits, advising on and reviewing data protection impacts and information sharing and investigating data breaches and incidents. They will also cooperate with, and be the key point of contact for, the Council's liaison with the Supervisory Authority (currently the UK Information Commissioner's Office).

Information Asset Owners

18. 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

19. 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.

Team / Service Managers

20. 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.

21. A role descriptor sets out in more detail the information governance responsibilities attributable to staff at each of these levels of the organisation.

Information Systems Owners

22. All information systems within the Council will have an assigned System Owner. Systems Owners are responsible for information systems. They will ensure system operating procedures are in place and are followed. They have responsibility to recognise actual or potential security incidents, consult their Information Asset Owners on incident management, and ensure that information systems are accurate and up to date.

23. All of the roles referenced above with a specific responsibility for information governance have an appropriate descriptor setting out responsibilities and expectations of the role.

Key governance bodies

24. The Information Governance Group (IGG) role and responsibilities include:

- Ensure a comprehensive and current Information Governance Framework is in place and operating effectively throughout the Council.
- Review and approve information governance procedures and standards.
- Lead the organisation's approach to controlling and managing information risk.
- Consider and address issues arising from reports of the Data Protection Officer.
- Coordinate information governance activities (data protection, information requests, security, quality, and records management) across the Council.
- Monitor information handling and breaches, implement assurance controls (including audits as required) and take corrective actions
- Ensure training and action plans for information governance are progressed throughout the Council and evaluate its impact and effectiveness.
- Communicate and champion the information governance agenda and the work of the Group.

25. The Group comprises the SIRO (Chair), Caldicott Guardians, Data Protection Officer, Senior Information Governance Advisor, representatives from Legal, Democratic Services and Complaints, Human Resources, Information and Community Technologies and each of the Departments within the Council.

Risk, Safety and Emergency Management Groups

26. Each Department has a Risk, Safety and Emergency Management Group whose role is to consider and address information governance risks within that Department, as part of a wider risk management agenda. The Group comprises senior staff from the relevant department, including the representative who will

also sit on the Information Governance Group, in order that there is a reporting and feedback link between the two Groups.

Resources

27. The Council has dedicated resources to support the implementation of its Information Governance Framework.

28. The Information Governance team will develop training and provide expert advice and guidance to all staff on Information Governance. It will develop, review and monitor compliance the Information Governance Framework of policies, standards and procedures and will support the DPO in carrying out their role.

29. The Complaints and Information team processes corporate information and Subject Access Requests, Freedom of Information requests and Environmental Information requests.

30. 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.

31. The Records Management Service 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.

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

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

34. 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.

35. There will be identified roles in the Groups whose role includes some aspects of information governance and ensuring compliance. These will vary according to the services provided.

General responsibilities

36. 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 guidelines within their directorates and services.

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

38. 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

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

40. 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,

41. Further modules, as appropriate, 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. The requirements and standards for these will be developed, agreed and kept under review.

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

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

44. 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.

45. Policies, procedures, standards and advice are available to staff at any time on the Information Management pages (LINK)

Monitoring and review

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

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

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

Further Information

49. Further Information

Details to be inserted upon approval

Appendices

External legislation

50. External legislation related to this policy includes

- General Data Protection Regulation (from 25 May 2018)
- Data Protection Act 1998 (to May 25 2018)
- Human Rights Act 1998
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Local Government Acts
- Copyright, Design and Patents Act 1998
- Computer Misuse Act 1990