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 personal, special category, sensitive and confidential information is effectively managed through clear accountability, governance processes, policies, training and appropriate resources.

## Information Governance Principles

5. The Council adopts the following core principles to underpin how information is managed across all services. These principles apply to all information, regardless of format or location:

    a) **Lawfulness, fairness and transparency** - Information is obtained, used and shared lawfully and clearly and be understandable to individuals.
    b) **Purpose limitation and data minimisation** - Information is only collected and used where necessary for defined purposes and is limited to what is required.
    c) **Accuracy and quality** - Information is maintained accurately, kept up to date and is fit for purpose.
    d) **Security and resilience** - Information is protected against unauthorised access, loss or damage through appropriate organisational and technical measures.
    e) **Information lifecycle management** - Information is managed from creation through to disposal in accordance with agreed standards, including retention and secure destruction.
    f) **Accountability and auditability** - The Council can demonstrate compliance with legal and regulatory requirements through clear ownership, audit trails and documentation.
    g) **Value and ethical use** - Information is recognised as a strategic asset and is used responsibly to support service delivery, insight and decision-making.

## Scope

6. 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.

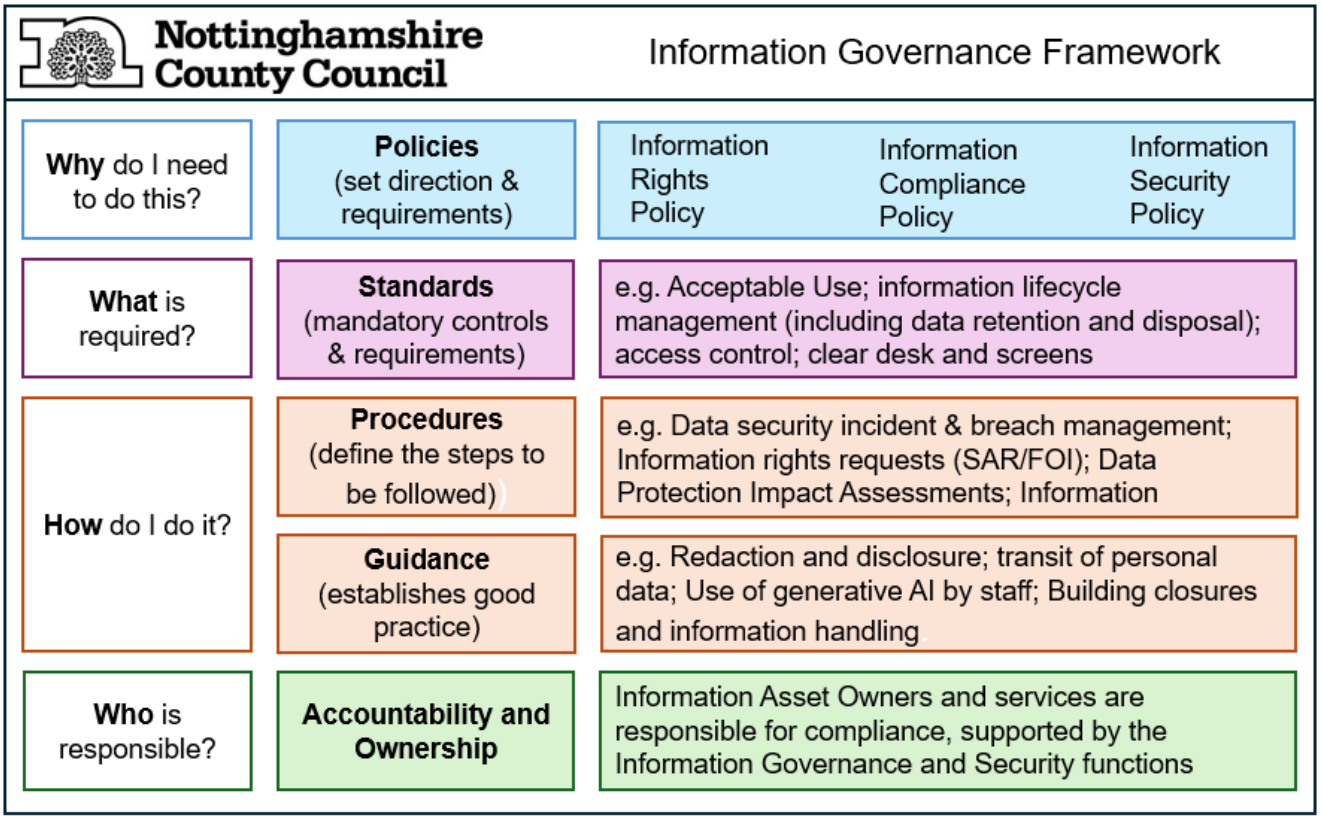
7. Schools are responsible for their own compliance with data protection and information legislation as independent data controllers.

## Key policies

8. 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 ICT specialist staff with information for staff distilled into the Acceptable Use Standard.

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



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

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

## Cabinet and Cabinet Members

12. The Council operates an Executive Leader and Cabinet model. Decisions are taken by the Cabinet and individually by Cabinet Members, as well as by authorised officers. Cabinet has responsibility for approving policies. Other important decisions relating to information governance are the responsibility of the Cabinet Member for Personnel.

## 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 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. 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 and Cyber Security 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
    - gives strategic direction to the work of the Data Protection Officer (DPO)

Caldicott Guardian

16. All NHS organisations and local authorities which provide social care must have a Caldicott Guardian. The Caldicott Guardian in the Council is appointed by the Corporate Leadership Team and is typically a Service Director in the Adult Social Care or Children and Families Departments. They are supported in their work by a deputy(s).

17. The Caldicott Guardian is 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 to ensure people's information is kept confidential and used appropriately).

Data Protection Officer

18. All public authorities handling large volumes of personal data must appoint a Data Protection Officer (DPO). The DPO must act independently and is responsible for advising on data protection obligations, monitoring compliance, supporting DPIAs, investigating breaches, and acting as a contact for individuals and the Information Commissioner's Office (ICO), which is the UK Regulator for Data Protection.

19. Within the Council, the DPO is also the Senior Responsible Owner for ensuring the compliant use of CCTV and other surveillance systems in line with relevant legislation and the Surveillance Camera Code of Practice.

20. Details of the current SIRO, Caldicott Guardian and DPO role holders is made available on the Council's intranet at Information governance responsibilities and role descriptions.

Information Asset Owners

21. Each Service Director (or equivalent senior manager) acts as an Information Asset Owner (IAO) and is accountable for the information assets within their area. This includes ensuring risks are identified and managed, information is used appropriately, and compliance with this framework is maintained. Expectations for this role are supported through targeted information risk training and guidance.

22. IAOs may delegate day-to-day responsibilities to appropriate managers within their services but remain accountable for ensuring that information governance requirements are met.

23. For the purposes of this framework, 'information assets' include the information, systems and processing activities recorded within the Council's Information and Processing Register (IPR).

Heads of Service, Service and Team Managers

24. Heads of Service, Service and Team Managers are responsible for understanding how information, particularly personal and other sensitive information is used within their area. They support IAOs in identifying, managing and mitigating information risks, and ensuring compliance with information governance requirements. This includes promoting good practice among staff, completing relevant information risk training

targeted at managers, using available guidance and checklists, and supporting the prevention and management of data breaches.

25. Information Risk: Training and Guides for Information Asset Owners (IAOs) and Managers sets out the mandatory training requirements for Service Directors (IAOs), Heads of Service, and Service and Team Managers, supported by concise guidance materials.

Information Systems Owners

26. All information systems within the Council that collect, store or use personal data must have an assigned System Owner. System Owners are responsible for ensuring that appropriate operating procedures are in place to control and secure data, including effective access controls so that only authorised users can access information appropriate to their role, and that these are followed. They must ensure Data Protection Impact Assessments are completed where required, identify and respond to actual or potential security incidents and breaches, liaise with relevant Information Asset Owners where appropriate, and ensure that data within systems is accurate and kept up to date.

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

## Key officer governance bodies

Information Governance and Cyber Security Board

28. The Information Governance and Cyber Security Board (IGCSB) comprises the SIRO (Chair), Caldicott Guardian, the Data Protection Officer, senior representatives from Legal Services, ICT and Assurance. The role of the Board is to

- Promote the optimisation of the value of the Council's information assets;
- Foster a culture across the Council that values, protects, uses and shares information.
- Set principles and direction to ensure that information and data is managed with the same determination and focus as other key business objectives
- Ensure proportionate and effective compliance and business continuity regimes are in place to reduce the information and data related risks to the Council and data subjects;
- Monitor information governance and cyber security KPIs and mandate remediation actions required.

Emergency Management

29. The Emergency Management Board (EMB) is Nottinghamshire County Council's strategic group responsible for overseeing and coordinating the Council's emergency

planning, business continuity and resilience arrangements. It meets regularly to review the Council's preparation for emergencies and to ensure that effective plans, capabilities and response frameworks are in place.

30. Each department has a Risk, Safety and Emergency Management Group (or equivalent) to oversee these matters at a departmental level.

## Officer Resources

31. 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.

Information Governance Team

32. The IG 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).

Complaints and Information Team

33. 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.

ICT Security team

34. The ICT 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.

Records and information management function

35. The Council has a records and information management function to ensure that information is effectively managed across its lifecycle, regardless of format. This function is delivered through a combination of:

    a) a contracted Records Management Service, provided by Inspire, which manages the storage and handling of physical records
    b) the Information Governance function, which provides oversight, standards and guidance for the management of digital records and broader information lifecycle requirements.

36. Together, these arrangements ensure that records are appropriately created, stored, accessed, retained and disposed of in a consistent and compliant manner.

37. Responsibility for applying records management standards rests with services and Information Asset Owners, who must ensure that information is managed in line with Council requirements.

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

39. 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 ICT Security teams.

40. The Business Intelligence Unit provides advice and guidance on data quality and more technical aspects of data minimisation (i.e. anonymisation and pseudonymisation).

41. 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

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

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

44. Wilful or negligent disregard for information governance policies, standards 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.

## Emerging information governance risks, opportunities and technologies

45. The Council recognises that the way information is created, used and shared continues to evolve. Emerging technologies and data practices introduce new risks and opportunities that must be managed appropriately. These include:

    - increased use of cloud-based systems and Software as a Service (SaaS)
    - data matching, analytics and business intelligence activities
    - artificial intelligence and automated decision-making tools

- increased data sharing across organisations and partnerships

46. The Council will ensure that appropriate governance controls, including Data Protection Impact Assessments (DPIAs), security measures and ethical considerations, are applied to these activities.

## Training and guidance

47. The Council will ensure that all staff and those acting on its behalf receive appropriate training and awareness in information governance, including data protection, information security and information rights.

48. Training requirements are defined through the Council's Information Governance Training Needs Assessment and related standards, with compliance monitored through corporate governance arrangements.

## Monitoring and review

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

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

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

## Supporting Policies

52. The primary appendices of this policy document are the Information Rights; Compliance and Security Policies. Each of these policies has a list of standards, procedures and guidance documents which are available at the time of approval and can be found in the Information Governance Policy Library.

## External Legislation

53. The Council will ensure that its approach to information governance reflects current legislation and enables the responsible and lawful use of data, including data sharing and access where appropriate.

- UK Data Protection Regulation (GDPR)
- Data Protection Act 2018
- Data (Use and Access) Act 2025
- Human Rights Act 1998
- Protection of Freedoms Act 2012

- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Computer Misuse Act 1990

## Further Information

54. 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, Temporary IG Programme Advisor |
| **Approver** | Senior Information Risk Owner (SIRO) under delegation from Policy Committee |
| **Date of Approval** | 06/08/2026 |
| **Date of next review** | 07/08/2028 |
| **Version** | 2.4 |
| **Classification** | Public |

| Version | Date | Changes |
|---|---|---|
| 1.0 | 28/03/2018 | Original document approved by Policy Committee based on a framework originally developed by Warwickshire County Council. |
| 2.0 | 30/10/2019 | Changes to reflect post-GDPR experience, framework diagram, governance changes, insert links etc. Approved by SIRO under delegation from Policy Committee |
| 2.1 | 17/01/2023 | General review and minor changes to include revised roles; team names etc and to update links. |
| 2.2 | 27/11/2023 | Minor changes to reflect NCC's change in corporate governance and revised terms of reference for the Information Governance and Cyber Security Board. |
| 2.3 | 16/04/2026 | Review and minor amends including to training section. |
| 2.4 | 06/08/2026 | Minor changes to add principles, emerging risks / opportunities, some organisational structural changes to roles. |